HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

Tiedekunta – Fakultet – Faculty	Koulutusohjelma – Utbildningsprogram – Degree programme	
Matemaattis-luonnontieteellinen	Matematiikka, aineenopettajan koulutus	
Tekijä – Författare – Author		
Tuukka Ylinampa		
Työn nimi – Arbetets titel – Title		
Ketjuehtorenkaat		
Työn laji – Arbetets art – Level	Aika – Datum – Month and year	Sivumäärä – Sidoantal – Number of pages
Pro gradu -tutkielma	Elokuu 2018	46 sivua

Tiivistelmä – Referat – Abstract

Tämä pro gradu –tutkielma käsittelee rengasteorian osa-alueita renkaiden alkeista ketjuehtorenkaiden ominaisuuksiin. Ketjuehtorenkailla tarkoitetaan renkaita, jotka toteuttavat nousevan tai laskevan ketjun ehdon. Nousevan ketjun ehdon toteuttavat renkaat ovat Noetherin renkaita ja laskevan ketjun ehdon toteuttavat renkaat ovat Artinin renkaita. Tutkielmalla on kaksi päämäärää, joista ensimmäinen on esitellä ja tutkia ketjuehtorenkaita. Toinen päämäärä on koota ehyt kokonaisuus erilaisista renkaista ja renkaisiin liittyvistä rakenteista. Tutkielmassa esitellään monia rengasteorian rakenteita ja tutkitaan niiden välisiä yhteyksiä.

Tutkielman ensimmäinen luku on johdantoa, minkä jälkeen toisessa luvussa käsitellään renkaita, kokonaisalueita ja kuntia. Kolmas luku keskittyy renkaiden ideaaleihin, tekijärenkaisiin ja pääideaalialueisiin. Neljännessä luvussa määritellään alkuideaalit, maksimaaliset ideaalit sekä tekijöihinjaon alueet. Viides luku käsittelee ketjuehtorenkaita eli Noetherin ja Artinin renkaita. Tässä luvussa käydään läpi Hilbertin kantalauseen todistus. Hilbertin kantalauseen mukaan polynomirengas on Noetherin rengas, jos sen kerroinrengas on noetherilainen. Kuudennessa luvussa jatketaan ketjuehtorenkaiden käsittelyä sekä todistetaan, että jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue. Kuudennessa luvussa kootaan myös tutkielmassa käsitellyt rengasrakenteet sisältymisen mukaiseen järjestykseen.

Lukijalle riittää esitiedoiksi perusteet lukualueista, laskutoimituksista ja ryhmäteoriasta.

Avainsanat – Nyckelord – Keywords

Rengasteoria, Noetherin rengas, Artinin rengas, pääideaalialue, yksikäsitteisen tekijöihinjaon alue

Säilytyspaikka – Förvaringställe – Where deposited

Kumpulan tiedekirjasto

Muita tietoja – Övriga uppgifter – Additional information

Ketjuehtorenkaat

Tuukka Ylinampa

26.08.2018

Sisältö

Luku 1

Johdanto

Tämä tutkielma käsittelee rengasteorian osa-alueita renkaiden alkeista ketjuehtorenkaiden ominaisuuksiin. Rengasteoria on abstraktin algebran tutkimusalue, johon kuuluu lukuisia aiheita. Tässä työssä tutkitaan renkaisiin liittyviä lauseita ja tuloksia. Tutkielmalla on kaksi päämäärää, joista ensimmäinen on esitellä sekä tutkia ketjuehtorenkaita. Toinen päämäärä on koota ehyt kokonaisuus erilaisista renkaista ja renkaisiin liittyvistä rakenteista. Ketjuehtorenkaat ovat kuitenkin suurimmassa roolissa tässä tutkielmassa, minkä vuoksi tutkielma on nimetty niiden mukaan. Ketjuehtorenkailla tarkoitetaan renkaita, jotka toteuttavat nousevan tai laskevan ketjun ehdon. Nousevan ketjun ehdon toteuttavat renkaat ovat Noetherin renkaita ja laskevan ketjun ehdon toteuttavat renkaat ovat Artinin renkaita.

Tutkielman alkupuolella käsitellään laajasti renkaita ja niiden ideaaleja. Nämä perusteet on välttämätöntä käydä läpi, jotta ketjuehtorenkaiden tutkiminen on mielekästä. Samalla tutustutaan erilaisiin rengaskenteisiin. Tutkielmassa esitellään monia rengasteorian rakenteita ja tutkitaan niiden välisiä yhteyksiä. Tutkielman loppupuolella käsitellään Noetherin ja Artinin renkaita sekä tutkitaan lisää tutkielmassa käsiteltyjen rakenteiden yhteyksiä.

Tutkielman ensimmäisessä matemaattisessa luvussa eli tutkielman toisessa luvussa tarkastellaan renkaita, kokonaisalueita ja kuntia. Lisäksi luvussa luodaan katsaus polynomeihin ja polynomirenkaisiin. Renkaat esitellään useiden esimerkkien avulla. Kokonaisalueista ja kunnista todistetaan yleisiä tuloksia, joita hyödynnetään myöhemmin tutkielmassa.

Tutkielman kolmas luku käsittelee renkaiden ideaaleja. Yksi luvun aiheista on tekijärengas, joka määritellään ideaalien avulla. Lisäksi luvussa käsitellään ideaalien virittämistä. Kolmannessa luvussa esitellään virittämisen avulla määriteltävät pääideaalirengas ja pääideaalialue. Pääideaalialue on yksi rengasteorian tärkeistä rengasrakenteista, joita tutkielmassa tutkitaan tarkemmin.

Neljäs luku lähestyy renkaita ja ideaaleja hieman toisesta suunnasta. Luvussa käsitellään jaollisuutta ja tekijöihinjakoa renkaiden kannalta. Luvun aluksi määritellään alkuideaali ja maksimaalinen ideaali. Näiden ideaalien avulla voidaan todistaa erilaisia tuloksia muun muassa tekijärenkaisiin liittyen. Luvussa käsitellään myös alkualkioiden ja jaottomien lukujen käyttäytymistä kokonaisalueissa ja pääideaalialueissa. Lisäksi luvussa määritellään yksikäsitteisen tekijöihinjaon alue. Yksikäsitteisen tekijöihinjaon alue on yleisempi käsite kuin pääideaalialue tai kunta. Tämän tuloksen todistaminen ei ole vielä tämän luvun työkaluilla mahdollista, joten todistukseen palataan kuudennessa luvussa.

Viidennessä luvussa tutkitaan Noetherin ja Artinin renkaita eli ketjuehtorenkaita. Luvussa määritellään laskevan ja nousevan ketjun ehdot, ideaalien minimi- ja maksimiehdot sekä Noetherin ja Artinin renkaat. Lisäksi luvussa todistetaan, että jokainen pääideaalialue on Noetherin alue sekä merkittävä tulos Hilbertin kantalause. Hilbertin kantalauseen mukaan polynomirengas on noetherilainen, jos sen kerroinrengas on noetherilainen.

Kuudennessa luvussa jatketaan ketjuehtorenkaiden tutkimista. Luvussa todistetaan Noetherin ja Artinin renkaille päteviä tuloksia. Luvussa todistetaan rakenteiden välisten yhteyksien kannalta tärkeä tulos, jonka mukaan jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue. Tämän myötä täydennetään rakenteiden välisten sisältymisten ketjua.

Lukijan esitiedoiksi riittää laskutoimitusten ja ryhmäteorian perusteet. Lisäksi tutkielmassa sivutaan kompleksilukuja sekä homomorfismia, joita ei käsitellä perusteistä lähtien.

Luku 2

Renkaat ja kokonaisalueet

Tämä luku käsittelee *renkaita*, *kokonaisalueita* ja *kuntia*. Ensiksi määritellään rengas joka on tutkielman olennaisimpia käsitteitä. Seuraavaksi siirrytään kokonaisalueisiin ja kuntiin. Luvussa todistetaan, että jokainen kunta on kokonaisalue ja jokainen äärellinen kokonaisalue on kunta. Lisäksi luvussa käydään läpi *polynomeja* sekä määritellään *polynomirengas*. Tämän jälkeen todistetaan, että kokonaisalueesta muodostettu polynomirengas on kokonaisalue. Luvussa on käytetty lähteinä enimmäkseen kirjoja [2] ja [3] ja [5].

Rengas on algebrallinen rakenne, jossa on määritelty kaksi erillistä laskutoimitusta, joita kutsutaan yleensä yhteen- ja kertolaskuksi. Renkaan laskutoimitukset toimivat keskenään osittelulakien mukaan.

Määritelmä 2.1. *Rengas* $(R, *, \circ)$ koostuu epätyhjästä joukosta R, jolle on määritelty kaksi erillistä laskutoimitusta $*$ ja $\circ$ siten, että:

1. pari $(R, *)$ on *vaihdannainen ryhmä*
2. pari $(R, \circ)$ on *monoidi*
3. kaikilla $a, b, c \in R$ pätevät *osittelulait*:

$$(a * b) \circ c = (a \circ c) * (b \circ c)$$
$$c \circ (a * b) = (c \circ a) * (c \circ b)$$

Kuten edellä mainittiin renkaan laskutoimitusta $*$ kutsutaan yleensä *yhteenlaskuksi* $(+)$ ja laskutoimitusta $\circ$ *kertolaskuksi* $(\cdot)$. Renkaaseen $(R, *, \circ)$ voidaan viitata symbolilla R renkaan joukon mukaan, jos tunnetaan kyseisen renkaan laskutoimitukset. Avaamalla ryhmän ja monoidin käsitteet rengas voidaan määritellä ehtojen avulla kuten seuraavassa määritelmässä.

Määritelmä 2.2. Rengas on epätyhjä joukko R, jolle on määritelty yhteenlasku $+$ ja kertolasku $\cdot$ siten, että kaikilla $a, b, c \in R$ pätevät:

1. $a + (b + c) = (a + b) + c$ ja $a(bc) = (ab)c$
2. $a + b = b + a$
3. on olemassa $0 \in R$, jolle pätee $a + 0 = 0 + a = a$ ja $1 \in R$, jolle pätee $a1 = 1a = a$
4. kaikille $a \in R$ löytyy $-a$, siten, että $a + (-a) = (-a) + a = 0$
5. $a(b + c) = ab + ac$ ja $(b + c)a = ba + ca$

Yhteenlasku on renkaan määritelmän mukaan vaihdannainen ja renkaan alkioilla on sen suhteen käänteisalkiot, joita kutsutaan *vasta-alkioksi*. Yhteenlaskun neutraalialkiota 0 sanotaan *nolla-alkioksi*.

Kertolaskun neutraalialkiota 1 kutsutaan puolestaan *ykkösalkioksi*. Kertolaskun ollessa vaihdannainen, kyseessä on *vaihdannainen rengas*. Lisäksi, jos vaihdannaisen renkaan alkioilla, nolla-alkiota lukuunottamatta, on käänteisalkiot myös kertolaskun suhteen, eli pari $(R \setminus \{0\}, \cdot)$ on vaihdannainen ryhmä, kyseessä on *kunta*, joka määritellään tarkemmin myöhemmin.

Renkaan määritelmästä seuraa yksinkertaisia, mutta hyödyllisiä tuloksia, jotka muistuttavat kokonaislukujen laskusääntöjä.

Lause 2.3. *Kaikilla renkaan alkioilla $a, b \in R$ pätevät seuraavat ehdot:*

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = (ab)$

Todistus. Todistetaan ehto kerrallaan. Oletetaan, että $a, b \in R$.

1. Yhteenlaskun neutraalialkiolle eli nolla-alkiolle pätee $0 = 0 + 0$. Täten

$$\begin{aligned} & 0 \cdot a \\ & = (0 + 0) \cdot a \\ & = 0 \cdot a + 0 \cdot a \\ \Leftrightarrow\ & 0 \cdot a - (0 \cdot a) = 0 \cdot a + 0 \cdot a - (0 \cdot a) \\ \Leftrightarrow\ & 0 = 0 \cdot a. \end{aligned}$$

Samalla tavoin osoitetaan $a \cdot 0 = 0$.

2. Käyttämällä edellistä tulosta ja osittelulakia saadaan

$$\begin{aligned} 0 &= 0 \cdot b \\ &= (a + (-a))b \\ &= ab + (-a)b. \end{aligned}$$

Tästä nähdään, että $(-a)b$ on alkion ab vasta-alkio eli

$$(-a)b = -(ab).$$

Jälleen samalla periaatteella saadaan osoitettua, että $a(-b) = -(ab)$

3. Käyttämällä 2. kohdan tulosta saadaan:

$$\begin{aligned} (-a)(-b) &= -((-a)b) \\ &= -(-(ab)) \\ &= ab \end{aligned}$$

□

Esimerkkejä renkaista ovat muun muassa kokonaislukurengas $(\mathbb{Z}, +, \cdot)$, reaalilukujen rengas $(\mathbb{R}, +, \cdot)$, rationaalilukujen rengas $(\mathbb{Q}, +, \cdot)$ ja kompleksilukujen rengas $(\mathbb{C}, +, \cdot)$, jotka kaikki ovat varustettu yhteen -ja kertolaskulla. Lisäksi jäännösluokkien joukko $\mathbb{Z}_n$ on rengas $(\mathbb{Z}_n, +, \cdot)$, kun yhteen- ja kertolasku määritellään seuraavalla tavalla kaikille $[a]_n, [b]_n \in \mathbb{Z}_n$:

$$\begin{aligned} [a]_n + [b]_n &= [a + b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n. \end{aligned}$$

Kaikki edellä mainitut renkaat ovat vaihdannaisia, koska reaali- ja kompleksilukujen yhteen- ja kertolasku ovat vaihdannaisia laskutoimituksia. Eräs esimerkki renkaista on myös reaaliarvoisten funktioiden joukko $F(\mathbb{R}) = \{f \in F(\mathbb{R}) \mid f(a) \in \mathbb{R}, \text{ kaikilla } a \in \mathbb{R}\}$. Renkaan $(F(\mathbb{R}), +, \cdot)$ laskutoimitukset ovat määritelty seuraavasti:

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x) \end{aligned}$$

kaikilla $f, g \in F(\mathbb{R})$.

Renkaat voivat muodostua myös polynomeista. Tällaisia renkaita käsitellään myöhemmin lisää.

Tavallisin esimerkki epävaihdannaisesta renkaasta on $n \times n$ -neliömatriisien joukko $M_n(\mathbb{R})$ varustettuna matriisien yhteen- ja kertolaskulla, kun $n \geqslant 2$. Epävaihdannaisuus seuraa suoraan matriisien kertolaskusta, joka ei ole vaihdannainen.

Esimerkki 2.4. Todistetaan, että kompleksilukurengas $\mathbb{C}$ on todella rengas. Kompleksilukujen yhteenlasku määritellään kaavalla

$$\begin{aligned} & x + y \\ &= (a + bi) + (c + di) \\ &= (a + c) + (b + d)i \end{aligned}$$

ja kompleksilukujen kertolasku määritellään kaavalla

$$\begin{aligned} & xy \\ &= (a + bi)(c + di) \\ &= ac + adi + bci + bdi^2 \\ &= (ac - bd) + (ad + bc)i. \end{aligned}$$

Todistetaan, että kompleksiluvut varustettuna kompleksilukujen yhteen- ja kertolaskulla on rengas käymällä läpi määritelmän 2.2. ehdot.

1. Olkoot x, y ja z kompleksilukuja. Tällöin $x = a+bi$, $y = c+di$ ja $z = e+fi$, joillain $a, b, c, d, e, f \in \mathbb{R}$ ja i on imaginaariyksikkö.

   Kompleksilukujen yhteenlaskun liitännäisyys seuraa kompleksilukujen yhteenlaskun määritelmästä ja reaalilukujen yhteenlaskun liitännäisyydestä:

$$\begin{aligned} & x + (y + z) \\ &= (a + bi) + ((c + di) + (e + fi)) \\ &= (a + bi) + ((c + e) + (d + f)i) \\ &= (a + (c + e)) + (b + (d + f))i \\ &= ((a + c) + e) + ((b + d) + f)i \\ &= ((a + c) + (b + d)i) + (e + fi) \\ &= ((a + bi) + (c + di)) + (e + fi) \end{aligned}$$

$$= (x + y) + z.$$

Samoin kompleksilukujen kertolaskun liitännäisyys seuraa kompleksilukujen kertolaskun määritelmästä ja reaalilukujen kertolaskun liitännäisyydestä:

$$\begin{aligned}
& x(yz) \\
&= (a + bi)((c + di)(e + fi)) \\
&= (a + bi)((ce - df) + (cf + de)i) \\
&= (a(ce - df) - b(cf + de)) + (a(cf + de) + b(ce - df))i \\
&= (ace - adf - bcf - bde) + (acf + ade + bce - bdf)i \\
&= ((ac - bd)e - (ad + bc)f) + ((ac - bd)f + (ad + bc)e)i \\
&= ((ac - bd) + (ad + bc)i)(e + fi) \\
&= ((a + bi)(c + di))(e + fi) \\
&= (xy)z.
\end{aligned}$$

2. Olkoot $x, y \in \mathbb{C}$. Tällöin $x = a + bi$ ja $y = c + di$, joissa $a, b, c, d \in \mathbb{R}$. Kompleksilukujen yhteenlasku on vaihdannainen, koska reaalilukujen yhteenlasku on vaihdannainen:

$$\begin{aligned}
& x + y \\
&= (a + bi) + (c + di) \\
&= (a + c) + (b + d)i \\
&= (c + a) + (d + b)i \\
&= (c + di) + (a + bi) \\
&= y + x.
\end{aligned}$$

3. Kompleksilukujen yhteenlaskun neutraalialkio on $0 = 0 + 0i$, sillä kaikilla kompleksiluvuilla $x = a + bi$, jossa $a, b \in \mathbb{R}$, pätee

$$\begin{aligned}
& x + 0 \\
&= (a + bi)(0 + 0i) \\
&= (a + 0) + (b + 0)i \\
&= a + bi \\
&= x
\end{aligned}$$

ja

$$0 + x = x.$$

Jälkimmäinen ehto seuraa kompleksilukujen yhteenlaskun vaihdannaisuudesta.

Kompleksilukujen kertolaskun neutraalialkio on $1 = 1 + 0i$, koska kaikilla kompleksiluvuilla $x = a + bi$, jossa $a, b \in \mathbb{R}$, pätee

$$\begin{aligned} & 1 \cdot x \\ &= (1 + 0i)(a + bi) \\ &= a + bi + 0 \cdot ai + 0 \cdot bi^2 \\ &= a + bi \\ &= x \end{aligned}$$

ja

$$\begin{aligned} & x \cdot 1 \\ &= (a + bi)(1 + 0i) \\ &= a + a \cdot 0i + bi + b \cdot 0i^2 \\ &= a + bi \\ &= x. \end{aligned}$$

4. Jokaisella kompleksiluvulla on vasta-alkio yhteenlaskun suhteen, koska jokaisella reaaliluvulla on vastaluku yhteenlaskun suhteen. Olkoon $x \in \mathbb{C}$, jolloin $x = a + bi$, joillain $a, b \in \mathbb{R}$. Tällöin $-x = -a - bi$ on kompleksiluvun x vasta-alkio, koska

$$\begin{aligned} & x + (-x) \\ &= (a + bi) + (-a - bi) \\ &= (a - a) + (b - b)i \\ &= 0 + 0i \\ &= 0 \end{aligned}$$

ja

$$-x + x = 0.$$

Jälkimmäinen ehto seuraa taas kompleksilukujen yhteenlaskun vaihdannaisuudesta.

5. Viimeisenä todistetaan, että kompleksiluvuilla ja niiden laskutoimituksilla pätee osittelulait. Olkoot $x, y, z \in \mathbb{C}$. Tällöin $x = a + bi$, $y = c + di$ ja $z = e + fi$, joissa $a, b, c, d, e, f \in \mathbb{R}$. Kompleksiluvuille pätee

$$\begin{aligned}
&x(y+z)\\
&= (a+bi)((c+di)+(e+fi))\\
&= (a+bi)((c+e)+(d+f)i)\\
&= (a(c+e)-b(d+f))+(a(d+f)+b(c+e))i\\
&= (ac+ae-bd-bf)+(ad+af+bc+be)i\\
&= ((ac-bd)+(ae-bf))+((ad+bc)+(af+be))i\\
&= ((ac-bd)+(ad+bc)i)+((ae-bf)+(af+be)i)\\
&= (a+bi)(c+di)+(a+bi)(e+fi)\\
&= xy+xz.
\end{aligned}$$

   Myös toinen osittelulaki

$$(y+z)x = yx + yz$$

   pätee. Todistus etenee samaan tapaan kuin ylhäällä. Toinen osittelulaki seuraa myös siitä, että kompleksilukujen kertolasku on vaihdannainen. Todistetaan kertolaskun vaihdannaisuus seuraavaksi. Kompleksiluvuilla pätee yleisesti

$$\begin{aligned}
&xy\\
&= (a+bi)(c+di)\\
&= (ac-bd)+(ad+bc)i\\
&= (ca-db)+(da+cb)i\\
&= (ca-db)+(cb+da)i\\
&= (c+di)(a+bi)\\
&= yx.
\end{aligned}$$

   Nyt on todistettu, että kompleksilukujen joukko varustettuna kompleksilukujen yhteen- ja kertolaskulla on vaihdannainen rengas.

Jos renkaan nolla-alkio ja ykkösalkio ovat sama alkio, kyseessä on *nollarengas*, jonka ainoa alkio on 0, ja jolle pätee: $0 + 0 = 0$ ja $0 \cdot 0 = 0$.

Määritellään seuraavaksi kaksi rengasta tarkempaa käsitettä, *kokonaisalue* ja *kunta*. Kokonaisalue on vaihdannainen rengas, jossa ei ole *nollanjakajia*.

Määritelmä 2.5. Vaihdannainen rengas D on kokonaisalue, jos kaikilla renkaan D nollasta poikkeavilla alkiolla a, b pätee

$$ab \neq 0.$$

Kuten edellä sanottiin kokonaisalue on vaihdannainen rengas, jossa ei ole nollanjakajia. Renkaan alkio $a \neq 0$ on nollanjakaja, jos sille pätee $ab = 0$ ja $ac = 0$, joillakin nollasta poikkeavilla $b, c \in R$. Kokonaisalueen määritelmän ehto voidaan myös ilmaista muodossa

$$ab = 0 \quad \Leftrightarrow \quad a = 0 \; tai \; b = 0.$$

Kokonaisalueessa D pätee supistussääntö. Tämä tarkoittaa, että yhtälöstä $ab = ac$ seuraa $b = c$, kaikilla $a, b, c \in D$ ja $a \neq 0$.

Edellä mainitut vaihdannaiset renkaat $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ ja $\mathbb{Z}$ ovat kokonaisalueita. Esimerkki vaihdannaisesta renkaasta, joka ei ole kokonaisalue, on jäännösluokkarengas $\mathbb{Z}_n$ kun n on yhdistetty luku eli luku, jolla on useampi tekijä kuin 1 tai luku itse. Esimerkiksi vaihdannaisen renkaan $\mathbb{Z}_6$ nollasta poikkeavien alkioiden $[2]_6$ ja $[3]_6$ tulolle pätee

$$[2]_6 \cdot [3]_6 = [2 \cdot 3]_6 = [6]_6 = [0]_6.$$

Niinpä $\mathbb{Z}_6$ ei ole kokonaisalue. Myöskään nollarengas ei ole kokonaisalue.

Seuraavaksi tarkasteltava käsite on kunta. Kunta on vaihdannainen rengas, jonka jokaisella nollasta poikkevalla alkiolla on käänteisalkio kertolaskun suhteen. Renkaan alkiota, jolla on käänteisalkio kertolaskun suhteen, sanotaan *yksiköksi*. Siten kunta on vaihdannainen rengas, jonka jokainen nollasta poikkeava alkio on yksikkö. Kunta voidaan määritellä renkaan määritelmää 2.1. muistuttavalla tavalla.

Määritelmä 2.6. Kunta K on epätyhjä joukko, jolle pätee:

1. pari $(K, +)$ on vaihdannainen ryhmä
2. pari $(K, \cdot)$ on vaihdannainen ryhmä
3. kaikilla $a, b, c \in K$ pätevät *osittelulait*:

$$(a + b)c = ac + bc$$
$$c(a + b) = ca + cb$$

Kokonaisluvut $\mathbb{Z}$ eivät ole kunta, koska kaikille kokonaisluvuille ei löydy kokonaislukujen joukosta käänteisalkiota kertolaskun suhteen. Sen sijaan rationaaliluvut $\mathbb{Q}$, reaaliluvut $\mathbb{R}$ ja kompleksiluvut $\mathbb{C}$ ovat kuntia.

Esimerkki 2.7. Jatketaan kompleksilukujen käsittelyä ja osoitetaan, että kompleksilukurengas $\mathbb{C}$ on kunta.

Esimerkissä 2.4. todistettiin, että kompleksiluvut varustettuna kompleksilukujen yhteen- ja kertolaskulla muodostavat vaihdannaisen renkaan. Tällöin kunnan määritelmän täyttymistä varten täytyy enää todistaa, että jokainen nollasta poikkeava kompleksiluku on yksikkö.

Oletetaan, että $z \in \mathbb{C}$. Tällöin $z = a + bi$, joillain $a, b \in \mathbb{R}$. Osoitetaan, että luku

$$z^{-1} = \frac{a - bi}{a^2 + b^2}$$

on luvun z käänteisalkio kompleksilukujen kertolaskun suhteen. Luku z^{-1} on todella kompleksiluku, koska reaaliluvuilla on käänteisalkiot kertolaskun suhteen ja reaalilukujen summat, tulot ja neliöt ovat reaalilukuja. Koska kompleksiluvuille z ja z^{-1} pätee

$$\begin{aligned} & zz^{-1} \\ &= (a + bi)\frac{a - bi}{a^2 + b^2} \\ &= \frac{(a + bi)(a - bi)}{a^2 + b^2} \\ &= \frac{a^2 - abi + abi - bi^2}{a^2 + b^2} \\ &= \frac{(a^2 + b^2) + (-ab + ab)i}{a^2 + b^2} \\ &= 1 + 0i \\ &= 1 \end{aligned}$$

ja

$$z^{-1}z = 1 + 0i = 1,$$

jokainen nollasta poikkeava kompleksiluku on yksikkö. Jälkimmäinen ehto seuraa kompleksilukujen kertolaskun vaihdannaisuudesta. Koska jokainen nollasta poikkeava kompleksiluku on yksikkö, kompleksilukurengas $\mathbb{C}$ on kunta.

Kokonaisalue on kuntaa yleisempi käsite eli kaikki kunnat ovat kokonaisalueita. Kaikki kokonaisalueet eivät ole kuitenkaan kuntia. Ainoastaan kokonaisalueet, joilla on rajallinen määrä alkioita, voivat olla kuntia. Itse asiassa kaikki äärelliset kokonaisalueet ovat kuntia. Todistetaan seuraavaksi nämä tulokset.

Lause 2.8. *Olkoon K kunta. Tällöin K on kokonaisalue.*

Todistus. Todistuksessa tarvitsee vain osoittaa, että kunnassa ei ole nollanjakajia. Olkoon K kunta. Tällöin K on vaihdannainen rengas. Olkoot $a, b \in K$ ja $ab = 0$. Oletetaan nyt, että $a \neq 0$ ja $b \neq 0$. Tällöin alkiolla a on kunnassa K käänteisalkio a^{-1}. Tutkitaan nyt yhtälöä $ab = 0$. Kertomalla yhtälöä alkiolla a^{-1} saadaan $b = 0$, mistä seuraa ristiriita. Siispä $a = 0$ tai $b = 0$ ja edelleen K on kokonaisalue. □

Lause 2.9. *Kokonaisalue D, jossa on äärellinen määrä alkioita, on kunta.*

Todistus. Olkoon D äärellinen kokonaisalue eli vaihdannainen rengas, jossa ei ole nollanjakajia. Näytetään toteen, että kaikilla kokonaisalueen D nollasta poikkeavilla alkiolla on käänteisalkio. Olkoon a kokonaisalueen D nollasta poikkeava alkio.

Tutkitaan kaikki tuloja ar, jossa $r \in D$. Oletetaan, että $ar = ax$, jollain $x \in D$. Tällöin $a(r - x) = 0$ ja edelleen $r = x$, koska kokonaisalueessa D ei ole nollanjakajia. Tästä seuraa, että kun $r \neq x$, niin $ar \neq ax$. Niinpä jokainen tulo ar on erillinen.

Koska D on äärellinen, tuloja ar on tasan yhtä monta kuin kokonaisalueen D alkioita. Niinpä kaikki kokonaisalueen D alkiot, ykkösalkio mukaanlukien, esiintyvät tulojen ar joukossa. Toisin sanoen $ar = 1$, sopivalla alkiolla r. Tämä todistaa, että r on alkion a käänteisluku ja edelleen, että kokonaisalue D on kunta. □

Esitellään vielä eräs rengastyyppi, jota käsittelemme myöhemmin lisää. Vaihdannaisen renkaan yli otetut *polynomit* muodostavat *polynomirenkaan*, kun polynomeille on määritelty laskutoimitukset summalle ja tulolle. Pohjustetaan polynomirengas polynomien käsittelyllä.

Yhden muuttujan polynomi määritellään yleensä summana

$$\sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

jossa a_k on polynomin *kerroin* eli *kertoja*, x on *tuntematon* eli *muuttuja* ja n on *polynomin aste*. Kertoimen ja muuttujan tuloa, eli polynomin jonkin asteista osaa, sanotaan *termiksi*. Polynomin summa voitaisi ajatella myös äärettömänä. Tällöin kaikkien termien, joiden aste on korkeampaa kuin polynomin aste, kertoimet ovat nollia.

Olkoot f ja g polynomeja, tällöin niiden summa ja tulo näyttävät seuraavilta

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$$

$$= \sum_{k=0}^{\infty} (a_k + b_k)^k$$

ja

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots$$
$$= \sum_{k=0}^{\infty}(\sum_{i+j=k} a_ib_j)x^k.$$

Summat ovat äärettömiä, koska summapolynomin tai tulopolynomin termien määrä riippuu summan tai tulon jäsenpolynomeista. Jälleen summapolynomin tai tulopolynomin astetta korkeampien termien kertoimet ovat nollia.

Määritellään seuraavaksi kaksi polynomeihin liittyvää funktiota, joita käytetään lisää myöhemmin.

Määritelmä 2.10. Merkintä $kor(f)$ tarkoittaa polynomin f korkeimman asteen termin kerrointa.

Esimerkiksi polynomille $f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ funktio kor on

$$kor(f) = a_n.$$

Määritelmä 2.11. Merkintä $deg(f)$ tarkoittaa polynomin astetta.

Esimerkiksi polynomille $f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ funktio deg on

$$deg(f) = n.$$

Määritelmä 2.12. Olkoon R vaihdannainen rengas. Tällöin polynomit, joiden kertoimet kuuluvat renkaaseen R, muodostavat polynomirenkaan $R[X]$.

Vaihdannaista rengasta, johon polynomirenkaan polynomien kertoimet kuuluvat, kutsutaan *kerroinrenkaaksi*. Polynomirengas voi periä kerroinrenkaan ominaisuuksia. Esimerkiksi kokonaisalueesta muodostettu polynomirengas on kokonaisalue. Todistetaan seuraavaksi tämä tulos.

Lause 2.13. *Olkoon D kokonaisalue. Kokonaisalueesta D muodostettu polynomirengas $D[X]$ on kokonaisalue.*

Todistus. Oletetaan, että D on kokonaisalue ja $D[X]$ siitä muodostettu polynomirengas. Olkoot f ja g renkaan $D[X]$ nollasta poikkeavia alkioita. Nyt polynomit f ja g ovat muotoa

$$f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

ja

$$g = b_mx^m + b_{m-1}x^{n-1} + \cdots + b_1x + b_0,$$

missä $a_n \neq 0$ ja $b_m \neq 0$. Polynomin f aste on nyt n ja polynomin g aste on nyt m. Polynomien f ja g tulo on

$$fg = a_n b_m x^{n+m} + \cdots + (a_0 b_1 + a_1 b_0)x + a_0 b_0.$$

Koska D on kokonaisalue, pätee $a_n b_m \neq 0$. Tästä seuraa, että $fg \neq 0$. Nyt, koska ehdosta $f, g \neq 0$ seuraa $fg \neq 0$, polynomirengas $D[X]$ on kokonaisalue. □

Edellisen lauseen todistuksesta saadaan myös toinen tulos. Nollasta poikkeavien polynomien f ja g tulon fg aste on polynomien asteiden summa. Muotoillaan tämä korollaariksi deg-funktion avulla.

Korollaari 2.14. *Olkoot f ja g polynomirenkaan $D[X]$ nollasta poikkeavia polynomeja. Lisäksi olkoon kerroinrengas D kokonaisalue. Tällöin $deg(fg) = deg(f) + deg(g)$.*

Luku 3

Ideaalit

Tässä luvussa esitellään *ideaalit*, *tekijärengas* ja *pääideaalit*. Aluksi käydään läpi renkaan ideaalia esimerkkien avulla. Sitten esitellään ideaalien sivuluokkien avulla määriteltävä tekijärengas. Tekijärengas todistetaan renkaaksi, minkä jälkeen siirrytään käsittelemään ideaalien virittämistä. Luvussa keskitytään yhden alkion virittämiin ideaaleihin eli pääideaaleihin. Luvun lopussa määritellään pääideaalien avulla tärkeät rakenteet *pääideaalirengas* ja *pääideaalialue*. Luvussa todistetaan myös, että jokainen kunta on pääideaalirengas. Luvussa on käytetty lähteinä kirjoja [1], [2] ja [4].

Renkailla on erilaisia käytännöllisiä osajoukkoja ja alirakenteita. Yksi erityisen käyttökelpoinen käsite on *ideaali*, joka vastaa melko analogisesti ryhmälle määriteltyä *normaalia aliryhmää*. Ideaali on renkaan osajoukko, jonka alkiot muodostavat renkaan aliryhmän yhteenlaskun suhteen. Lisäksi ideaali on on suljettu renkaan alkiolla kerrottaessa, eli minkä tahansa renkaan alkion ja ideaalin alkion tulo kuuluu ideaaliin.

Määritelmä 3.1. Renkaan R osajoukkoa I kutsutaan ideaaliksi, jos sille pätee:

1. Pari $(I, +)$ on aliryhmä ryhmälle $(R, +)$.
2. Kaikilla $r \in R$ ja $a \in I$ pätee $ra \in I$ ja $ar \in I$.

Jos renkaan osajoukko I on on ryhmän $(R, +)$ aliryhmä ja sille pätee kaikilla $r \in R$ ja $a \in I$ vain toisen ehdon toinen puoli $ar \in I$, sitä kutsutaan renkaan *vasemmanpuoleiseksi ideaaliksi*. Samaan tyyliin määritellään renkaan *oikeanpuoleinen ideaali* osajoukoksi I, joka on ryhmän $(R, +)$ aliryhmä, jolle pätee vain toisen ehdon osuus $ra \in I$, kaikilla $r \in R$ ja $a \in I$. Vaihdannaisilla renkailla toinen ehto toteutuu, jos, kaikilla $a \in I$ ja $r \in R$, toinen tuloista ra tai ar kuuluu ideaaliin I.

Määritelmän 3.1. toteuttavia osajoukkoja kutsutaan myös *kaksipuolisiksi ideaaleiksi*, mutta tässä tutkielmassa niistä puhutaan yksinkertaisesti ideaaleina.

Määritelmästä seuraa, että rengas R on itsensä ideaali. Renkaan aitoja ideaaleja ovat kuitenkin vain joukot, jotka ovat renkaan aitoja osajoukkoja. Lisäksi määritelmän mukaan joukko $\{0\}$ on renkaan R ideaali, jota sanotaan *nollaideaaliksi*. Näitä kahta erikoistapausta kutsutaan renkaan *triviaaleiksi ideaaleiksi*.

Huomautetaan, että ideaali ei yleensä sisällä renkaan ykkösalkiota. Renkaan ykkösalkio kuuluu ainoastaan triviaaliin ideaaliin R, mikä todistetaan seuraavaksi.

Lause 3.2. *Olkoon R rengas ja I renkaan R ideaali. $R = I$, jos ja vain jos $1 \in I$.*

Todistus. Oletetaan, että I on renkaan R ideaali ja $1 \in I$. Määritelmän mukaan kaikilla $r \in R$ pätee nyt

$$1 \cdot r = r \in I.$$

Tästä seuraa, että $R \subset I$. Toisaalta tiedetään, että $I \subset R$, joten $I = R$.

Oletaan, että I on renkaan R ideaali ja $I = R$. Tällöin $1 \in I$ renkaan määritelmän mukaan. □

Esimerkki 3.3. Kokonaislukurenkaan $\mathbb{Z}$ ideaalit ovat muotoa $n\mathbb{Z}$, jossa $n \in \mathbb{Z}$. Tämä seuraa siitä, että renkaan $\mathbb{Z}$ ideaalin täytyy olla ryhmän $(\mathbb{Z}, +)$ aliryhmä ja *syklisen ryhmän*, jollainen $(\mathbb{Z}, +)$ on, aliryhmät ovat muotoa $n\mathbb{Z}$. [2 korollaari 9.10. s. 129] Osoitetaan nyt, että $n\mathbb{Z}$ on kokonaislukurenkaan $\mathbb{Z}$ ideaali kaikilla $n \in \mathbb{Z}$.

Aiemmin todettiin, että $n\mathbb{Z}$ on joukon $\mathbb{Z}$ aliryhmä yhteenlaskun suhteen. Näyetään vielä, että $ar \in n\mathbb{Z}$ kaikilla $a \in n\mathbb{Z}$ ja $r \in \mathbb{Z}$. Tämä riittää todistamaan määritelmän 3.1. toisen ehdon, sillä tiedetään, että $\mathbb{Z}$ on vaihdannainen rengas. Olkoot $n \in \mathbb{Z}$, $a \in n\mathbb{Z}$ ja $r \in \mathbb{Z}$. Tällöin

$$a = nk$$

jollain $k \in \mathbb{Z}$ ja edelleen

$$ar = nkr.$$

Koska $kr \in \mathbb{Z}$ kaikilla $k, r \in \mathbb{Z}$, $ar \in n\mathbb{Z}$ kaikilla $n \in \mathbb{Z}$. Niinpä $n\mathbb{Z}$ on kokonaislukurenkaan $\mathbb{Z}$ ideaali. Niinpä renkaan $\mathbb{Z}$ ideaalit ovat muotoa $n\mathbb{Z}$, jossa $n \in \mathbb{Z}$.

Esimerkki 3.4. Edellisen luvun alussa käsitellyllä kuvausrenkaalla

$$F(\mathbb{R}) = \{f \in F(\mathbb{R}) \mid f(a) \in \mathbb{R}\ \forall a \in \mathbb{R}\}$$

on ideaali, joka muodostuu kuvauksista, jotka kuvaavat kaikki lähtöjoukon alkiot nolla-alkioksi. Tällaisia kuvauksia sanotaan nollakuvauksiksi. Todistetaan, että joukon $F(\mathbb{R})$ osajoukko

$$N(\mathbb{R}) = \{f \in F(\mathbb{R}) \mid f(a) = 0\ \forall a \in \mathbb{R}\}$$

on kuvausrenkaan $(F(\mathbb{R}), +, \cdot)$ ideaali.

Olkoot $f, g \in N(\mathbb{R})$. Tällöin $f(a) = 0$ ja $g(b) = 0$ kaikilla $a, b \in \mathbb{R}$.

1. Joukko $N(\mathbb{R})$ on vakaa yhteenlaskun suhteen, sillä

$$\begin{aligned} & f+g \\ &= f(a)+g(b) \\ &= 0+0=0, \end{aligned}$$

kaikilla $f, g \in N(\mathbb{R})$ ja $a, b \in \mathbb{R}$.

Yhteenlaskun neutraalialkio 0 kuuluu joukkoon $N(\mathbb{R})$, koska

$$0 = f(a) \in N(\mathbb{R})$$

kaikilla $a \in \mathbb{R}$.

Lisäksi kaikilla joukon $F(\mathbb{R})$ alkioilla on vasta-alkiot yhteenlaskun suhteen. Esimerkiksi g on alkion f vasta-alkio, sillä

$$\begin{aligned} & f+g \\ &= f(a)+g(b) \\ &= 0+0=0 \end{aligned}$$

ja yhteenlasku on vaihdannainen. Kaikki aliryhmäehdot pätevät, joten pari $(N(\mathbb{R}),+)$ on parin $(F(\mathbb{R}),+)$ aliryhmä.

2. Kaikilla $f \in N(\mathbb{R})$ ja $g \in F(\mathbb{R})$ pätee $fg \in N(\mathbb{R})$ ja $gf \in N(\mathbb{R})$, koska

$$\begin{aligned} & fg \\ &= fg(a) \\ &= f(a)g(a) \\ &= 0 \cdot g(a) = 0 \end{aligned}$$

ja

$$\begin{aligned} & gf \\ &= gf(a) \\ &= g(a)f(a) \\ &= g(a) \cdot 0 = 0 \end{aligned}$$

kaikilla $a, b \in \mathbb{R}$ ja nollakuvaukset kuuluvat joukkoon $N(\mathbb{R})$. Niinpä joukko $N(\mathbb{R})$ on renkaan $F(\mathbb{R})$ ideaali määritelmän 3.1. mukaan.

Ideaalit voivat määrittää renkaaseen liittyvän tekijärakenteen. Renkaan R ideaali I voi määrittää ideaalin sivuluokkien joukon, jota merkitään R/I. Sivuluokassa renkaan R alkioon r summataan ideaalin alkiot $a \in I$. Sivuluokka on siten muotoa

$$r + I = \{r + a \mid a \in I\}.$$

Renkaan R ideaalin I sivuluokkien muodostamaa joukkoa kutsutaan *tekijärenkaaksi.*

Määritelmä 3.5. Olkoon R rengas, jolla on ideaali I. Tekijärengas on joukko R/I, jonka laskutoimitukset ovat

$$(a + I) + (b + I) = (a + b) + I,$$
$$(a + I)(b + I) = ab + I,$$

kaikilla $a, b \in R$.

Lause 3.6. *Tekijärengas R/I on rengas.*

Todistus. Tekijärenkaan laskutoimitukset pätevät kuten renkaan laskutoimitukset, koska ne palautuvat renkaan laskutoimituksiin. Olkoot $a, b, c \in R$.

Todistetaan määritelmän 2.1. ensimmäinen ehto, eli että R/I on vaihdannainen ryhmä yhteenlaskun suhteen. Koska $(I, +)$ on ryhmän $(R, +)$ normaali aliryhmä, $(R/I, +)$ on ryhmä. Ryhmän $(R/I, +)$ vaihdannaisuus seuraa ryhmän $(R, +)$ vaihdannaisuudesta:

$$\begin{aligned}(a + I) + (b + I) \\ = (a + b) + I \\ = (b + a) + I \\ = (b + I) + (a + I)\end{aligned}$$

kaikilla $a, b \in R$.

Ryhmän nolla-alkio on sivuluokka $I = 0 + I$, koska

$$\begin{aligned}(a + I) + (0 + I) \\ = (a + 0) + I \\ = a + I\end{aligned}$$

kaikilla $a \in R$ ja yhteenlasku on vaihdannainen.

Sivuluokan $(a + I)$ vasta-alkio on sivuluokka $(-a + I)$, koska

$$(a + I) + (-a + I)$$

$$= (a - a) + I$$
$$= 0 + I = I$$

kaikilla $a \in R$ ja yhteenlasku on vaihdannainen.

Määritelmän 2.1. toinenkin ehto toteutuu renkaalta R periytyvillä ominaisuuksilla. Pari $(R/I, \cdot)$ on liitännäinen, koska renkaan R kertolasku on liitännäinen:

$$(a + I)((b + I)(c + I))$$
$$= (a + I)(bc + I)$$
$$= abc + I$$
$$= (ab + I)(c + I)$$
$$= ((a + I)(b + I))(c + I)$$

kaikilla $a, b, c \in R$.

Kertolaskun neutraalialkio on sivuluokka $1 + I$, koska

$$(1 + I)(a + I)$$
$$= 1a + I$$
$$= a + I$$

ja

$$(a + I)(1 + I)$$
$$= a1 + I$$
$$= a + I$$

kaikilla $a \in R$.

Myöskin renkaan määritelmän 2.1. kolmas ehto seuraa renkaan R ominaisuuksista. Tekijärenkailla pätevät osittelulait, koska reaaliluvuilla pätevät osittelulait:

$$(a + I)((b + I) + (c + I))$$
$$= (a + I)((b + c) + I)$$
$$= a(b + c) + I$$
$$= (ab + ac) + I$$
$$= (ab + I) + (ac + I)$$
$$= ((a + I)(b + I)) + ((a + I)(c + I))$$

ja

$$\begin{aligned}
&((a+I)+(b+I))(c+I)\\
&=((a+b)+I)(c+I)\\
&=(a+b)c+I\\
&=(ac+bc)+I\\
&=(ac+I)+(bc+I)\\
&=((a+I)(c+I))+((b+I)(c+I))
\end{aligned}$$

kaikilla $a, b, c \in R$.

Tekijärengas R/I on nyt renkaan määritelmän mukaan rengas. □

Seuraavaksi esitellään muutama ideaaleihin liittyvä yleinen tulos. Renkaan ideaalien leikkaus on myös kyseisen renkaan ideaali.

Lause 3.7. *Olkoon A satunnainen joukko renkaan R ideaaleja. Näiden ideaalien leikkaus $M = \bigcap_i A_i$ on renkaan R ideaali.*

Todistus. Olkoon $\{A_i\}$ renkaan R ideaaleista koostuva joukko ja M leikkaus kyseisistä joukosta, $M = \bigcap_i A_i$. Koska nolla-alkio kuuluu jokaiseen ideaaliin A_i, se kuuluu myös leikkaukseen M, joten $M \neq \emptyset$. Oletetaan, että $a, b \in M$ ja $r \in R$. Tällöin $a - b \in A_i$ ja $ar \in A_i$ kaikilla i, mistä seuraa, että $a - b \in M, ar \in M$, joten M on renkaan R ideaali. □

Ryhmäteoriasta tuttua alirakenteiden virittämistä esiintyy myös renkaissa. Ideaali voi olla jonkin renkaan alkion tai osajoukon virittämä.

Määritelmä 3.8. Olkoon R rengas, jolla on osajoukko $A = \{r_1, r_2, ..., r_n\}$. Kaikkien ideaalien $I_1, I_2, ..., I_n$, joille pätee $A \subset I_i$, leikkausta $\bigcap_i I_i$ sanotaan osajoukon A *äärellisesti virittämäksi ideaaliksi.*

Kun puhutaan äärellisestä virittämisen yhteydessä tarkoitetaan virittäjäalkioiden määrän äärellisyyttä.

Lause 3.9. *Osajoukon A virittämä ideaali $\langle A \rangle = \langle r_1, r_2, ..., r_n \rangle$ on pienin ideaali, joka sisältää koko joukon A. Tällaista ideaalia $\langle A \rangle$ kutsutaan alkioiden $r_1, r_2, ..., r_n$* äärellisesti virittämäksi *ideaaliksi.*

Todistus. Olkoon $\langle A \rangle$ renkaan R osajoukon A virittämä ideaali. Olkoon I renkaan R ideaali, joka sisältää joukon A. Tällöin pätee myös $\langle A \rangle \subseteq I$. Tästä seuraa, että $\langle A \rangle$ on renkaan R pienin ideaali, joka sisältää joukon A. □

Määritelmä 3.10. Yhden alkion a virittämää ideaalia $\langle a \rangle$ kutsutaan *pääideaaliksi*.

Triviaalit ideaalit ovat pääideaaleja. Nollaideaali $\{0\}$ on alkion 0 virittämä. Rengas R on ykkösalkion eli kertolaskun neutraalialkion virittämä. Kun ykkösalkio kuuluu ideaaliin, ideaali on koko rengas, kuten aiemmin todettiin. Ykkösalkion virittämä ideaali näyttää lauseen 3.11. mukaan seuraavalta:

$$\langle 1 \rangle = \{1r \mid r \in R\} = R.$$

Määritelmä 3.11. Rengasta, jonka kaikki ideaalit ovat pääideaaleja sanotaan *pääideaalirenkaaksi*.

Lause 3.12. *Vaihdannaisen renkaan R pääideaali $\langle a \rangle$, jossa $a \in R$, on muotoa*

$$\langle a \rangle = \{ar \mid r \in R\}$$

Todistus. Olkoon R vaihdannainen rengas ja a sen alkio. Todistetaan ensiksi, että joukko $\langle a \rangle = \{ar \mid r \in R\}$ on renkaan R ideaali.

Olkoot $x, y \in \langle a \rangle$. Nyt alkiot $x, y \in R$ ja ovat muotoa as ja at, joillakin $s, t \in R$. Käytetään hyväksi tietoa renkaalle R pätevistä laskusäännöistä ja saadaan

$$\begin{aligned} & x + y \\ &= as + at \\ &= a(s + t). \end{aligned}$$

Tästä seuraa, että $x + y \in \langle a \rangle$, koska $s + t \in R$ kaikilla $s, t \in R$.

Yhteenlaskun neutraalialkio kuuluu joukkoon $\langle a \rangle$, koska $0 = a \cdot 0 \in \langle a \rangle$.

Lisäksi koska renkaan R alkiolla on vasta-alkiot renkaassa R, jokaisella alkiolla $x \in \langle a \rangle$ on vasta-alkio joukossa $\langle a \rangle$:

$$\begin{aligned} & a \cdot (-s) \\ &= -as \\ &= -x \in \langle a \rangle. \end{aligned}$$

Niinpä joukko $\langle a \rangle$ on aliryhmä renkaalle R yhteenlaskun suhteen.

Todistetaan vielä, että kaikilla $y \in \langle a \rangle$ ja $r \in R$ pätee $yr \in \langle a \rangle$, mikä riittää todistamaan, että $\langle a \rangle$ on ideaali, koska rengas R on vaihdannainen. Oletetaan, että $y \in \langle a \rangle$ ja $r \in R$. Nyt $y \in R$ ja $y = au$, jollain $u \in R$. Tulolle yr pätee

$$yr = aur.$$

Koska $u, r \in R$ niin $ur \in R$. Niinpä tulo yr kuuluu joukkoon $\in \langle a \rangle$. Nyt on todistettu, että $\langle a \rangle$ on renkaan R ideaali.

Olkoon nyt I renkaan R pienin ideaali, joka sisältää alkion a. Kuitenkin lauseen 3.8. mukaan $\langle a \rangle$ on pienin ideaali, joka sisältää alkion a. Näin ollen $I = \langle a \rangle = \{ar \mid r \in R\}$. $\square$

Esimerkissä 3.3. kävi ilmi, että kokonaislukurenkaan $\mathbb{Z}$ ideaalit ovat muotoa $n\mathbb{Z}$, jossa $n \in \mathbb{Z}$. Kaikki kokonoaislukurenkaan ideaalit ovat siten muotoa $\langle n \rangle$, eli yhden alkion virittämiä. Toisin sanoen kaikki kokonaislukurenkaan ideaalit ovat pääideaaleja, minkä johdosta $\mathbb{Z}$ on pääideaalirengas.

Todistetaan seuraavaksi, että jokainen kunta on pääideaalirengas. Tämä on seurausta siitä, että kunnilla on vain kaksi ideaalia, jotka ovat kunnan triviaalit ideaalit.

Lause 3.13. *Kunnan K ainoat ideaalit ovat K ja $\{0\}$.*

Todistus. Jokaisella kunnalla K on ideaalit K ja $\{0\}$. Lisäksi $K \neq \{0\}$, koska nollarengas ei ole kunta. Osoitetaan, että kunnalla K ei ole muita ideaaleja.

Olkoon $I \neq \{0\}$ kunnan K ideaali. Tällöin ideaalin I alkiolla $a \neq 0$ on kunnassa K käänteisalkio a^{-1}. Nyt ideaalin määritelmästä seuraa, että $aa^{-1} = 1 \in I$. Koska $1 = aa^{-1} \in I$, lauseen 3.2. mukaan $I = K$. Niinpä kunnassa K on vain triviaalit ideaalit $\{0\}$ ja K. □

Aiemmin näytettiin, että triviaalit ideaalit ovat pääideaaleja. Täten kunnan kaikki ideaalit ovat pääideaaleja ja edelleen jokainen kunta on pääideaalirengas.

Korollaari 3.14. *Olkoon K kunta. Tällöin K on pääideaalirengas.*

Määritelmä 3.15. Pääideaalirengas, joka on kokonaisalue määritellään *pääideaalialueeksi.*

Muistetaan edellisestä luvusta, että kokonaislukujen joukko $\mathbb{Z}$ on kokonaisalue. Koska $\mathbb{Z}$ on myös pääideaalirengas, kokonaislukurengas $\mathbb{Z}$ on pääideaalialue. Jokainen kunta on myös pääideaalialue, koska kunnat ovat pääideaalirenkaita ja lauseen 2.8. nojalla jokainen kunta on kokonaisalue.

Luku 4

Alkuideaalit, maksimaaliset ideaalit ja tekijöihinjako renkaissa

Tässä luvussa käydään läpi perusteita jaollisuudesta ja alkuluvuista renkaissa. Luvun alussa määritellään *alkuideaalit* ja *maksimaaliset ideaalit*, joiden avulla tutkitaan muun muassa tekijärenkaita. Luvussa todistetaan, että vaihdannaisen renkaan maksimaaliset ideaalit ovat alkuideaaleja. Lisäksi tässä luvussa tutkitaan jaottomien lukujen ja alkualkioiden käyttäytymistä kokonaisalueissa. Luvun lopuksi määritellään *yksikäsitteisen tekijöihinjaon alue*, jota käsitellään myöhemmin lisää. Tutkielmassa käsitellään alkuideaaleja ja maksimaalisia ideaaleja, koska niitä tarvitaan joissakin ketjuehtorenkaisiin liittyvissä todistuksissa. Luvun lähteinä on käytetty enimmäkseen kirjoja [6] ja [7].

Määritelmä 4.1. Olkoon R vaihdannainen rengas. Renkaan R nollasta poikkeava eikääntyvä alkio a on jaoton, jos aina kun

$$a = bc \text{ joillakin } b, c \in R,$$

toinen alkioista b tai c on yksikkö.

Määritelmä 4.2. Olkoon R vaihdannainen rengas ja a, b ja $p \neq 0$ sen alkioita. Luku p on alkualkio renkaassa R, jos aina kun

$$p|ab,$$

niin $p|a$ tai $p|b$.

Sanallisesti alkualkion määritelmä voidaan avata seuraavalla tavalla. Aina kun luku p jakaa tulon ab, luku p jakaa myös joko luvun a tai luvun b.

Ideaalien joukossa on *alkuideaaleja*, joilla on monia vastaavia ominaisuuksia kuin alkuluvuilla kokonaislukurenkaassa. Määritellään seuraavaksi alkuideaali vaihdannaisessa renkaassa.

Määritelmä 4.3. Olkoon R vaihdannainen rengas, jolla on aito ideaali I. Jos kaikilla $a, b \in R$ ehdosta $ab \in I$ seuraa $a \in I$ tai $b \in I$, niin I on alkuideaali.

Esimerkiksi kokonaislukujen joukossa ideaali $\langle 6 \rangle$ ei ole alkuideaali, sillä $2 \cdot 3 = 6 \in \langle 6 \rangle$, mutta $2 \notin \langle 6 \rangle$ ja $3 \notin \langle 6 \rangle$. Kokonaislukujen joukossa $\langle 5 \rangle$ on alkuideaali. Tämä johtuu siitä, että jos kahden alkion tulo on viidellä jaollinen, niin vähintään toisen tulon tekijöistä on oltava viidellä jaollinen. Kokonaislukujen joukossa alkuideaalit ovat pääideaaleja ja *maksimaalisia ideaaleja.*

Määritelmä 4.4. Olkoon I renkaan R aito ideaali. I on maksimaalinen ideaali, jos se ei sisälly kokonaan mihinkään toiseen renkaan R aitoon ideaaliin.

Kokonaislukujen joukossa ideaali $\langle 4 \rangle$ ei ole maksimaalinen ideaali, sillä aito ideaali $\langle 2 \rangle$ sisältää ideaalin $\langle 4 \rangle$. Toisaalta $\langle 3 \rangle$ ei sisälly kokonaan mihinkään kokonaislukualeen aitoon ideaaliin, joten $\langle 3 \rangle$ on kokonaislukurenkaan $\mathbb{Z}$ maksimaalinen ideaali.

Kokonaislukurenkaassa $\mathbb{Z}$ maksimaaliset ideaalit ovat alkualkioiden virittämiä pääideaaleja. Tämä seuraa siitä, että $\mathbb{Z}/n\mathbb{Z}$ on kunta silloin kun n on alkualkio. Todistetaan seuraavaksi täman tuloksen yleinen muoto. Todistusta varten tarvitaan seuraavaa apulausetta.

Lemma 4.5. *Olkoon R/I vaihdannainen tekijärengas ja $a + I$ sen nollasta poikkeava alkio. Tällöin joukko*

$$J = \{ar + s \mid r \in R, s \in I\}$$

on renkaan R ideaali.

Todistus. Olkoon R/I vaihdannainen tekijäregas ja $a \in R$, jolle pätee $a \neq 0$. Tällöin $a + I$ on renkaan R/I alkio. Olkoon $J = \{ar + s \mid r \in R, s \in I\}$ ja olkoot $x, y \in J$. Nyt $x = ar + s$ ja $y = at + u$, joillakin $r, t \in R$ ja $s, u \in I$. Tällöin summa

$$\begin{aligned} & x + y \\ &= ar + s + at + u \\ &= a(r + t) + s + u, \end{aligned}$$

kuuluu joukkoon J, koska $r + t \in R$ ja $s + u \in I$. Niinpä joukko J on vakaa yhteenlaskun suhteen.

Yhteenlaskun neutraalialkio 0 on joukossa J, koska 0 kuuluu sekä renkaaseen R, että ideaaliin I. Niinpä

$$a \cdot 0 + 0 = 0 \in J$$

Joukon J alkion $x = ar + s$ vasta-alkio on $-x = -ar - s$. Alkio $-x$ on joukossa J, koska alkion $r \in R$ vasta-alkio $-r$ kuuluu renkaaseen R ja alkion $s \in I$ vasta-alkio $-s$ kuuluu ideaaliin I. Lisäksi alkiolle $-x$ pätee

$$x + (-x)$$

$$= ar + s + (-ar - s) = 0$$

ja

$$-x + x$$

$$= -ar - s + ar + s = 0$$

joten se on alkion x vasta-alkio.

Niinpä ryhmä $(J, +)$ on ryhmän $(R, +)$ aliryhmä.

Seuraavaksi todistetaan, että kaikilla $z \in R$ ja $x \in J$ tulo xz kuuluu joukkoon J. Kuten edellä määritettiin niin $x = ar + s$, joillakin $r \in R$ ja $s \in I$. Koska

$$xz$$

$$= (ar + s)z$$

$$= arz + sz$$

ja $rz \in R$ sekä $sz \in I$, niin $xz \in J$ kaikilla $x \in J$ ja $z \in R$. Nyt joukko J on ideaalin määritelmän 3.1. mukaan renkaan R ideaali. □

Seuraavaksi tutkitaan miten tekijärengas määrittyy, kun se muodostetaan alkuideaalin tai maksimaalisen ideaalin avulla.

Lause 4.6. *Olkoon R vaihdannainen rengas ja I sen ideaali. Tekijärengas R/I on kunta, jos ja vain jos I on renkaan R maksimaalinen deaali.*

Todistus. Oletetaan, että I on vaihdannaisen renkaan R ideaali ja tekijärengas R/I on kunta. Tällöin jokainen tekijärenkaan nollasta poikkeava alkio on yksikkö. Oletetaan, että $I \subset I_1$, jossa I_1 on renkaan R ideaali. Tällöin ideaalista I_1 löytyy alkio a, joka ei kuulu ideaalin I. Nyt $a \neq 0$ ja edelleen $a + I \in R/I$. Koska R/I on kunta, on olemassa $b \in R$, jolle pätee

$$(a + I)(b + I) = ab + I = 1 + I.$$

Seurauksena $ab - 1 \in I$. Olkoon nyt $m = ab - 1$. Tästä seuraa, että $ab - m = 1$. Koska $ab \in I_1$ ja $m \in I_1$, niin $ab - m$ kuuluu ideaalin I_1. Toisin sanoen ykkösalkio $ab - m = 1$ kuuluu ideaaliin I_1. Tästä seuraa lauseen 3.2. mukaan, että $I_1 = R$, jolloin ideaalin I on oltava renkaan R maksimaalinen ideaali.

Oletetaan nyt, että I on vaihdannaisen renkaan R maksimaalinen ideaali. Olkoon $a+I$ renkaan R/I nollasta poikkeava alkio. Todistetaan, että on olemassa $b+I \in R/I$, jollain $b \in R$, jolle pätee

$$(a+I)(b+I) = ab+I = 1+I.$$

Toisin sanoen etsitään alkio $b \in R$, jolle pätee $ab-1 \in I$. Määritellään nyt renkaan R alkiosta koostuva joukko J:

$$J = \{ar+s | r \in R, s \in I\}.$$

Joukko J on lemman 4.5. mukaan renkaan R ideaali. Toisaalta huomataan, että maksimaalinen ideaali I sisältyy ideaaliin J, koska kaikki ideaaliin I alkiot kuuluvat joukon J määritelmän mukaan joukkoon J, kun $a \cdot 0 + s = s$, jossa $s \in I$. Lisäksi $J \neq I$, sillä $a = a \cdot 1 + 0 \in J$, mutta $a \notin I$, koska muutoin pätisi $a+I = I$. Niinpä, koska I on renkaan R maksimaalinen ideaali, se ei voi sisältyä mihinkään renkaan R aitoon ideaaliin. Tästä seuraa, että $J = R$. Tällöin erityisesti $1 \in J$ ja $1 = ab - m$, joillain $b \in R$ ja $m \in I$. Tästä seuraa, että $ab - 1 \in I$ eli $ab + I = 1 + I$. Niinpä $b+I$ on alkion $a+I$ käänteisalkio. Koska kaikille nollasta poikkeaville tekijärenkaan R/I alkiolle löytyy käänteisalkio, R/I on kunta. □

Lause 4.7. *Olkoon I vaihdannaisen renkaan R ideaali. Tekijärengas R/I on kokonaisalue, jos ja vain jos I on alkuideaali.*

Todistus. Vaihdannaisesta renkaasta R muodostettu tekijärengas R/I on vaihdannainen rengas. Todistetaan, että tekijärengas R/I ei sisällä nollanjakajia, jos ja vain jos I on alkuideaali. Olkoon $a+I$ ja $b+I$ renkaan R/I nollasta poikkeavia alkioita. Tällöin $a, b \notin I$. Nyt

$$(a+I)(b+I) = ab+I = 0+I,$$

jos ja vain jos $ab \in I$. Määritelmän 4.3. mukaan tämä on totta, jos ja vain jos ideaali I ei ole alkuideaali. Niinpä tekijärenkaalla R/I ei ole nollanjakajia, jos ja vain jos I on alkuideaali. □

Korollaari 4.8. *Olkoon R vaihdannainen rengas. Tällöin jokainen renkaan R maksimaalinen ideaali I on alkuideaali.*

Todistus. Olkoon I vaihdannaisen renkaan R maksimaalinen ideaali. Tällöin lauseen 4.6. nojalla R/I on kunta ja edelleen lauseen 2.8. mukaan kokonaisalue. Siispä I on lauseen 4.7. nojalla alkuideaali. □

Kokonaisalueissa alkualkioita ja jaottomia lukuja määritellään alkuideaalien ja maksimaalisten ideaalien avulla.

Lause 4.9. *Kokonaisalueessa D pätee seuraavat ehdot:*

1. *Alkio $p \neq 0$ on jaoton, jos ja vain jos $\langle p \rangle$ on pääideaalialueen D maksimaalinen ideaali.*

2. *Jokainen kokonaisalueen D alkualkio on jaoton.*

3. *Jos D on pääideaalialue, jokainen alueen D jaoton luku on alkualkio.*

Todistus. Todistetaan ehto kerrallaan.

1. Oletetaan, että D on pääideaalialue ja luku $p \neq 0 \in D$ on jaoton. Olkoon $q \in D$ ja $\langle q \rangle = I_1$ kokonaisalueen D pääideaali, joka sisältää pääideaalin $\langle p \rangle = I$. Koska pätee
$$p \in \langle p \rangle \subset \langle q \rangle,$$
niin alkiolle p pätee $p = qr$, jollakin $r \in D$. Tästä seuraa, että joko q tai r on yksikkö, koska p on oletuksen mukaan jaoton. Jos q on yksikkö, niin $\langle q \rangle = I_1 = D$ ja I on kokonaisalueen D maksimaalinen ideaali. Jos r on yksikkö, niin $q = r^{-1}p$ ja edelleen $q \in \langle p \rangle$. Koska $p \in I_1$ ja $q \in I$, joukot I_1 ja I ovat samat eli $I = I_1$. Niinpä ei ole ideaalia, johon I sisältyy vaan I on kokonaisalueen D maksimaalinen ideaali.

   Olkoon nyt D pääideaalialue ja $p \in D$. Oletetaan nyt, että ideaali $\langle p \rangle = I$ on kokonaisalueen D maksimaalinen ideaali. Todistetaan alkion p jaottomuus vastaoletuksella. Oletetaan, että p on jaollinen. Tällöin $p = ab$, joillakin ei-kääntyvillä alkiolla $a, b \in D$. Nyt alkion p virittämälle ideaalille pätee
$$\langle p \rangle \subseteq \langle a \rangle.$$
   Jos $\langle a \rangle = \langle p \rangle$, niin $a \in \langle p \rangle$. Tästä seuraa, että $a = pc$, jollakin $c \in D$. Kun tähän yhdistetään aiempi tulo $p = ab$, saadaan $p = pcb$. Koska D on kokonaisalue ja $p \neq 0$ päästään tulokseen
$$1 = cb.$$
   Tämä tarkoittaa, että b on yksikkö, mikä johtaa ristiriitaan.

   Jos $\langle a \rangle \neq \langle p \rangle$, niin $\langle p \rangle \subset \langle a \rangle$. Nyt koska a ei ole yksikkö, niin
$$\langle a \rangle \neq D.$$
   Tämä johtaa ristiriitaan, koska nyt ideaali $I = \langle p \rangle$ ei ole kokonaisalueen D maksimaalinen ideaali. Niinpä alkion p on oltava jaoton.

2. Olkoon D kokonaisalue ja $p \in D$ alkualkio. Jos p on jaollinen, niin on olemassa eikääntyvät alkiot $a, b \in D$, joille pätee $p = ab$. Nyt p jakaa alkion a tai p jakaa alkion b. Oletetaan, että p jakaa alkion a. Tällöin $pc = a$, jollakin $c \in D$. Yhdistämällä tämä aiempaan tulokseen saadaan

$$p = pcb$$

ja edelleen

$$1 = cb,$$

koska D on kokonaisalue ja $p \neq 0$. Tällöin b on yksikkö, mikä johtaa ristiriitaan. Jos oletetaan, että p jakaa alkion b päädytään samalla tapaa tietoon, että a on yksikkö ja edelleen ristriitaan. Niinpä alkion p on oltava jaoton.

3. Olkoon D pääideaalialue ja $p \in D$ jaoton. Oletetaan, että $p|ab$, joillakin $a, b \in D$. Jotta p olisi alkualkio, täytyy näyttää toteen, että $p|a$ tai $p|b$. Tämän lauseen ensimmäisestä ehdosta saadaan selville, että $I = \langle p \rangle$ on kokonaisalueen D maksimaalinen ideaali. Edelleen korollaarin 4.8. nojalla I on alkuideaali. Alkuideaalin määritelmästä seuraa nyt, että, jos $ab \in I$, niin $a \in I$ tai $b \in I$. Tällöin pätee joko $p|a$ tai $p|b$. Tästä seuraa suoraan, että p on alkualkio.

□

Edellisen lauseen nojalla alkuluvut ja jaottomat luvut ovat pääideaalialueessa sama asia. Alkuluvut ja jaottomat luvut eivät ole kuitenkaan yleisesti sama asia. Joissakin kokonaisalueissa jokainen alkualkio on jaoton, mutta jokainen jaoton luku ei ole välttämättä alkualkio. Esimerkiksi kokonaisalueessa $\mathbb{Z}[\sqrt{-5}]$ alkio 3 on jaoton, mutta se ei alkualkio. Todistetaan tämä seuraavaksi erillisenä esimerkkinä.

Esimerkki 4.10. Luku 3 on jaoton kokonaisalueessa $\mathbb{Z}[\sqrt{-5}]$ alkio, mutta se ei alkualkio samassa kokonaisalueessa. Joukko $\mathbb{Z}[\sqrt{-5}$ on kokonaisalue, koska kaikki sen alkiot kuuluvat kokonaisalueeseen $\mathbb{C}$, jota käsiteltiin aiemmin tutkielman toisessa luvussa. Joukon $\mathbb{Z}[\sqrt{-5}]$ alkiot ovat muotoa $a + b\sqrt{5}i$, jossa $a, b \in \mathbb{Z}$ ja i on imaginääriyksikkö. Alkio $3 = 3+0\sqrt{5}i$ on kokonaisalueessa $\mathbb{Z}[\sqrt{-5}]$ jaoton, koska ei ole olemassa kahta ei-kääntyvää alkiota $x, y \in \mathbb{Z}[\sqrt{-5}]$, joille pätee $xy = 3$. Todistetaan tämä väite. Todistuksessa käytetään funktiota $N : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}_{\geq 0}$, joka kuvaa alkion $a + b\sqrt{5}i = x \in \mathbb{Z}[\sqrt{-5}]$ seuraavalla tavalla:

$$\begin{aligned} N(x) &= N(a + b\sqrt{5}i) \\ &= (a + b\sqrt{5}i)(a - b\sqrt{5}i) \\ &= a^2 + 5b^2. \end{aligned}$$

Funktio N kuvaa siten alkion $x = a + b\sqrt{5}i$ itsensä ja liittolukunsa $\overline{x} = a - b\sqrt{5}i$ tuloksi. Funktion N kuva-alkiota kutsutaan normiksi.

Kaikilla $x, y \in \mathbb{Z}[\sqrt{-5}]$ pätee $N(x)N(y) = N(xy)$, koska

$$\begin{aligned}
&N(x)N(y)\\
&= (a^2 + 5b^2)(c^2 + 5d^2)\\
&= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2\\
&= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 + 10abcd - 10abcd\\
&= a^2c^2 - 10abcd + 25b^2d^2 + 5(a^2d^2 + 2abcd + b^2c^2)\\
&(ac - 5bd)^2 + 5(ad + bc)^2\\
&= N(ac - 5bd + (ad + bc)\sqrt{5}i)\\
&= N(ac + ad\sqrt{5}i + bc\sqrt{5}i + b\sqrt{5}i \cdot d\sqrt{5}i)\\
&= N((a + b\sqrt{5}i)(c + d\sqrt{5}i))\\
&= N(xy),
\end{aligned}$$

kaikilla $a, b, c, d \in \mathbb{Z}$.

Oletetaan, että $3 = xy$, joillakin $x, y \in \mathbb{Z}[\sqrt{-5}]$. Tällöin pätee

$$N(x)N(y) = N(xy) = N(3) = 9.$$

Tästä seuraa, että ei-kääntyvän luvun x normin $N(x)$ täytyy olla 1, 3 tai 9. Jos $N(x) = 1$, niin x on yksikkö. Jos $N(x) = 9$, niin $N(y) = 1$ ja edelleen y on yksikkö. $N(x)$ tai $N(y)$ ei voi myöskään olla 3, koska $N(x) = a^2 + 5b^2 > 3$ kaikilla $a, b \in \mathbb{Z}_{\geq 0}$. Niinpä luvulla 3 ei olemassa ei-kääntyviä tekijöitä ja se on jaoton.

Luku $3 \in \mathbb{Z}[\sqrt{-5}]$ ei ole kuitenkaan alkualkio koska se ei jaa kumpaakaan luvuista $2 + \sqrt{5}i$ tai $2 - \sqrt{5}i$, mutta jakaa niiden tulon $(2 + \sqrt{5}i)(2 - \sqrt{5}i) = 4 - 5i^2 = 4 + 5 = 9$.

Tässä luvussa käydään läpi vielä alueita, jotka määritellään tekijöihinjaon avulla. Näitä ovat *tekijöihinjaonalue* sekä *yksikäsitteinen tekijöihinjaonalue*.

Määritelmä 4.11. Olkoon a kokonaisalueen D nollasta poikkeava ei-kääntyvä alkio. Luvulla a on *alkutekijähajotelma* kokonaisalueessa D, jos alkio a voidaan ilmaista jaottomien lukujen äärellisenä tulona. Tällöin alkio $a \in D$ on muotoa

$$a = up_1p_2 \dots p_n,$$

jossa u on kokonaisalueen D yksikkö ja $p_1, p_2, \dots, p_n$ ovat kokonaisalueen D jaottomia alkioita.

Määritelmä 4.12. Olkoon D kokonaisalue, jossa kaikilla nollasta poikkeavilla ei-kääntyvillä alkiolla on alkutekijähajotelma alueessa D. Tällöin sanotaan, että D on *tekijöihinjaon alue*.

Määritelmä 4.13. Tekijöihinjaon alue D, jossa kaikkien alkioiden alkutekijähajotelma on yksikäsitteinen, määritellään *yksikäsitteisen tekijöihinjaoen alueeksi*. Yksikäsitteinen alkutekijähajotelma tarkoittaa, sitä että alkion

$$a = up_1p_2 \dots p_n$$

tekijöihinjako on ainutlaatuinen yksikköä ja jaottomien alkioiden järjestystä lukuunottamatta.

Myöhemmin tässä tutkielmassa todistetaan, että jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue. Koska lauseen 4.9. mukaan pääideaalialueessa alkuluvut vastaavat jaottomia lukuja, niin tällöin myös yksikäsitteisen tekijöihinjaon alueessa jaottomat luvut ja alkuluvut ovat sama asia. Huomautetaan kuitenkin, että jokainen yksikäsitteisen tekijöihinjaon alue ei ole pääideaalialue.

Aiemmin tarkasteltu kokonaislukujen joukko $\mathbb{Z}$ on yksikäsitteisen tekijöihinjaon alue. Tämä seuraa siitä, että *aritmetiikan peruslauseen* nojalla jokainen kokonaisluku $n > 1$, joka ei ole alkualkio, voidaan ilmaista yksikäsitteisesti alkualkioiden tai niiden vastalukujen tulona [1, lause 1.4.8. s. 46]. Niinpä jokaiselle nollasta poikkeavalle ei-kääntyvälle kokonaisluvulle löytyy yksikäsitteinen alkutekijähajotelma. Tästä johtuen kokonaislukurengas $\mathbb{Z}$ on määritelmän 4.13. mukaan yksikäsitteisen tekijöihinjaon alue. Aritmetiikan peruslausetta ei käsitellä tarkemmin tässä tutkielmassa.

Esimerkki 4.14. Näytetään toteen, että aiemmin käsitelty kokonaisalue $\mathbb{Z}[\sqrt{-5}]$ ei ole yksikäsitteisen tekijöihinjaon alue. Todistuksessa käytetään ylempänä määriteltyä normikuvausta $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_{\geq 0}$. Todistuksessa osoitetaan, että kokonaisalueessa $\mathbb{Z}[\sqrt{-5}]$ on nollasta poikkeava ei-kääntyvä alkio, jolle löytyy kaksi eri alkutekijähajotelmaa. Tätä varten osoitetaan ensin, että kokonaisalueessa $\mathbb{Z}[\sqrt{-5}]$ on vain kaksi yksikköä, jotka ovat 1 ja -1.

Olkoot $z, w \in \mathbb{Z}[\sqrt{-5}]$. Tällöin $z = a + b\sqrt{5}i$ ja $w = c + d\sqrt{5}i$, joillain $a, b, c, d \in \mathbb{Z}$. Oletetaan, että $zw = 1$. Tällöin

$$N(z)N(w) = N(zw) = N(1) = 1.$$

Tästä seuraa, että $N(z) = 1$ ja $N(w) = 1$, jos z on yksikkö. Niinpä $N(z) = a^2 + 5b^2 = 1$. Tämä on mahdollista vain silloin, kun $b = 0$ ja $a = 1$ tai $a = -1$. Täten kokonaisalueen $\mathbb{Z}[\sqrt{-5}]$ ainoat yksiköt ovat 1 ja -1.

Tutkitaan nyt kokonaisalueen $\mathbb{Z}[\sqrt{-5}]$ alkiota 9. Luku 9 voidaan ilmaista tulona $3 \cdot 3 = 9$ tai tulona $(2+\sqrt{5})(2-\sqrt{5})$. Kaikki alkiot 3, $2+\sqrt{5}$ ja $2-\sqrt{5}$ kuuluvat kokonaisalueeseen

$\mathbb{Z}[\sqrt{-5}]$. Aiemmin todistettiin, että luku 3 on jaoton kokonaisalueessa $\mathbb{Z}[\sqrt{-5}]$. Samalla tavoin voidaan näyttää, että $2+\sqrt{5}$ ja $2-\sqrt{5}$ ovat myös jaottomia.

Oletetaan, että $xy = 2+\sqrt{5}$, joillain ei-kääntyvillä alkiolla $x, y \in \mathbb{Z}[\sqrt{-5}]$. Tällöin

$$N(x)N(y) = N(xy) = N(2+\sqrt{5}) = 9.$$

Tällöin $N(x)$ on joko 1, 3 tai 9. Luku 1 ei ole mahdollinen, koska silloin $x = 1$ on yksikkö. Myöskään luku 9 ei ole mahdollinen, koska silloin $N(y) = 1$ ja $y = 1$ on yksikkö. Koska $a^2 + 5b^2 \neq 3$ millään $a, b \in \mathbb{Z}_{\geq 0}$, niin myöskään luku 3 ei voi olla minkään luvun normi. Niinpä $2+\sqrt{5}$ on jaoton. Samalla tavoin $2-\sqrt{5}$ voidaan todistaa jaottomaksi.

Niinpä luvulle 9 on olemassa kaksi erillistä alkutekijähajotelmaa, jotka ovat $9 = 3 \cdot 3$ sekä $9 = (2+\sqrt{5})(2-\sqrt{5})$. Tästä johtuen kokonaisalue $\mathbb{Z}[\sqrt{-5}]$ ei ole yksikäsitteisen tekijöihinjaon alue.

Luku 5

Ketjuehtorenkaat

Tämän luvun renkaat oletetaan vaihdannaisiksi, ellei toisin todeta. Tässä luvussa käsitellään *ketjuehtorenkaita* eli renkaita, joiden ideaalit toteuttavat nousevan tai laskevan ketjun ehdon. Tällaisten renkaiden ideaaliketjut kasvavat tai suppenevat vain tiettyyn rajaan asti. Tässä luvussa tutkitaan aluksi renkaita, jotka toteuttavat nousevan ketjun ehdon. Näitä renkaita kutsutaan *Noetherin renkaiksi*. Noetherin renkaat on nimetty matemaatikko Emmy Noetherin (1882-1935) mukaan.

Luvun aluksi määritellään nousevan ketjun ehto, Noetherin rengas, ideaalien maksimiehto ja Noetherin alue. Sen jälkeen todistetaan, että jokainen pääideaalialue on Noetherin rengas. Luvun tärkein tulos on *Hilberin kantalause*. Hilbertin kantalauseen mukaan polynomirengas on noetherilainen, jos sen kerroinrengas on Noetherin rengas.

Noetherin renkaiden käsittelyn jälkeen siirrytään tutkimaan Artinin renkaita. Ensiksi määritellään laskevan ketjun ehto, artinilaisuus ja *ideaalien minimiehto*. Sitten todistetaan, että rengas on artinilainen jos se toteuttaa ideaalien minimehdon. Tämän jälkeen todistetaan, että kokonaislukurengas ei ole Artinin rengas. Tämän luvun lähteitä ovat kirjat [1], [4] ja [6].

Määritelmä 5.1. Rengas R toteuttaa *nousevan ketjun ehdon*, jos mitä tahansa renkaan ideaaleja

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots$$

kohden on olemassa kokonaisluku n, siten että kaikilla $m \geq n$ pätee $I_m = I_n$.

Määritelmä 5.2. Rengas, joka toteuttaa nousevan ketjun ehdon määritellään *Noetherin renkaaksi*. Voidaan myös sanoa renkaan olevan *noetherilainen*.

Määritelmä 5.3. Rengas toteuttaa *ideaalien maksimiehdon*, jos kaikilla renkaan epätyhjillä ideaaleista koostuvilla joukoilla on *maksimialkio*. Maksimialkio on sellainen ideaali, joka ei sisälly kokonaan mihinkään muuhun kyseisen joukon ideaalin.

Seuraavaksi todistetaan, että Noetherin renkaissa toteutuu ideaalien maksimiehto ja että jokainen Noetherin renkaan ideaali on äärellisesti viritetty. Nämä kolme ehtoa ovat ekvivalentteja. Tällöin yhden ehdon pätemisestä seuraa, että muutkin ehdot pätevät.

Lause 5.4. *Olkoon R rengas. Tällöin seuraavat ehdot ovat yhtäpitäviä:*

1. *R on Noetherin rengas (määritelmä 5.2.)*
2. *Renkaassa R toteutuu ideaalien maksimiehto (määritelmä 5.3.)*
3. *Jokainen renkaan R ideaali on äärellisesti viritetty*

Todistus. Todistetaan lause 5.4. ehtojen järjestyksessä, eli $1 \Rightarrow 2$, $2 \Rightarrow 3$, $3 \Rightarrow 1$.

$1 \Rightarrow 2$ Olkoon R on noetherilainen ja F epätyhjä joukko renkaan R ideaaleja. Jos ideaali $I_1 \in F$ ei ole joukon maksimialkio, on olemassa $I_2 \in F$, jolle pätee $I_1 \subset I_2$. Samalla tavalla päätellään, että jos I_2 ei ole joukon maksimialkio, löytyy $I_3 \in F$, jolle pätee $I_2 \subset I_3$. Jatkamalla tätä menetelmää saadaan nousevien ideaalien ketju

$$I_1 \subset I_2 \subset I_3 \subset \cdots,$$

jonka kaikki ideaalit kuuluvat renkaaseen R. Jos oletetaan, että joukolla F ei ole maksimialkiota, yllä oleva ideaaliketju jatkuu äärettömästi. Tämä on kuitenkin ristiriidassa alkuoletuksen mukaan, koska Noetherin renkailla kaikki ideaalit toteuttavat nousevan ketjun ehdon, eli ideaalijonoilla on jokin raja, eivätkä ne kasva äärettömästi. Siispä joukossa R oltava maksimialkio.

$2 \Rightarrow 3$ Olkoon I renkaan R satunnainen ideaali. Määritetään nyt joukko äärellisesti virtettyjä ideaaleja

$$F = \{A \in R \mid \text{A on äärellisesti viritetty ja } A \subseteq I\}.$$

Joukko F ei ole tyhjä, koska siihen sisältyy ainakin $\{0\} \subseteq I$. Koska renkaassa R pätee ideaalien maksimiehto, joukosta F löytyy maksimialkio M. Joukon F määritelmän mukaan pätee $M \subseteq I$. Oletetaan, että $M \neq I$, mistä seuraa, että $M \subset I$. Nyt on olemassa alkio a, joka kuuluu ideaaliin I, mutta ei joukkoon M. Koska $M \in F$, niin M on äärellisesti viritetty. Olkoon $M = \langle a_1, a_2, \cdots, a_t \rangle$. Nyt löytyy kuitenkin äärellisesti viritetty ideaali

$$B = \langle a_1, a_2, \cdots, a_t, a \rangle,$$

jolle pätee $B \subseteq I$. Tällöin $B \in F$ ja $M \subset B$, mistä seuraa ristiriita, koska M on joukon F maksimialkio. Siispä $M = I$, mistä seuraa, että renkaan R satunnainen ideaali I on äärellisesti viritetty.

$3 \Rightarrow 1$ Olkoon $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ nouseva ketju renkaan R ideaaleja. Tällöin ideaali

$$I = \bigcup_{n=1}^{\infty} I_n$$

on renkaan R äärellisesti viritetty ideaali. Tällöin ideaali I on muotoa $I = \langle a_1, a_2, \ldots, a_r \rangle$. Nyt jokainen ideaalin I virittäjä a_t, jossa $1 \leq t \leq r$, kuuluu johonkin ideaaliketjun ideaaliin I_{it}. Olkoon nyt n indeksien i_t maksimi, jolloin jokainen virittäjä a_t kuuluu ideaaliin I_n. Tästä seuraa, että kaikilla $m \geq n$ pätee

$$I = \langle a_1, a_2, \ldots, a_r \rangle \subseteq I_n \subseteq I_m \subseteq I.$$

Niinpä ideaalit I, I_m ja I_n ovat yksi ja sama ideaali ja etenkin

$$I_m = I_n.$$

Eli tietyn pisteen jälkeen annettu ideaalien ketju lakkaa kasvamasta ja saavuttaa maksimikokonsa. Siispä rengas R on Noetherilainen. □

Esimerkki 5.5. Todistetaan seuraavaksi, että kokonaislukujen joukko $\mathbb{Z}$ on Noetherin rengas. Tämä tarkoittaa sitä, että kokonaislukujen joukossa $\mathbb{Z}$ kaikki nousevat ideaaliketjut saavuttavat lopulta maksimialkion, eli ideaaliketjut eivät voi kasvaa loputtomasti.

Olkoon

$$I_1 \subset I_2 \subset I_3 \subset \ldots.$$

nouseva ketju kokonaislukurenkaan $\mathbb{Z}$ ideaaleja. Ideaalit $I_1, I_2, \ldots$ ovat pääideaaleja, koska ne kuuluvat kokonaislukurenkaaseen, joka on pääideaalialue. Niinpä jokainen ketjun ideaali on yhden alkion virittämä. Ketjun perättäisten ideaalien $I_t = \langle a_t \rangle$ ja $I_{t+1} = \langle a_{t+1} \rangle$ virittäjäalkioille pätee $a_{t+1} | a_t$ eli ketjussa edempänä olevan ideaalin virittäjäalkio jakaa aieman ideaalin virittäjäalkion. Niinpä kaikki ketjun ideaalien virittäjät a_i, jossa $i > 1$, jakavat ketjun ensimmäisen ideaalin virittäjän a_1. Koska äärellisellä luvulla voi olla vain äärellinen määrä jakajia, jokaisella kokonaislukurenkaan nousevalla ideaaliketjulla voi olla vain äärellinen määrä nousevia ideaaleja. Toisin sanoen jokainen kokonaislukurenkaan ideaaliketju saavuttaa jossain kohtaa maksimialkion, jonka jälkeen ideaalit lakkaavat kasvamasta. Yksi esimerkki kokonaislukurenkaan kasvavasta ideaaliketjusta on

$$\langle 32 \rangle \subset \langle 16 \rangle \subset \langle 8 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle = \mathbb{Z}.$$

Luvun kaksi virittämä ideaali sisältyy ainoastaan ykkösalkion virittämään ideaaliin, joka on itse kokonaislukurengas.

Renkaiden lisäksi, on muita algebrallisia rakenteita, jotka voivat olla Noetherilaisia. Seuraavaksi käsittelemme *Noetherin alueita.*

Määritelmä 5.6. Kokonaisalue, jossa pätee yksikin lauseen 5.4. ehdoista, on *Noetherin alue.*

Osoitetaan seuraavaksi, että pääideaalialue on erikoistapaus Noetherin alueesta. Toisin sanoen Noetherin alue on yleinen tapaus pääideaalialueesta. Tätä tulosta sivuttiin jo esimerkin 5.5. käsittelyssä.

Lause 5.7. *Jokainen pääideaalialue on Noetherin alue.*

Todistus. Olkoon D pääideaalialue, johon kuuluu ideaaleja, jotka muodostavat nousevan ketjun

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots.$$

Olkoon $I = \bigcup_r I_r$, joka on nyt myös pääideaalialueen D ideaali. Koska D on pääideaalialue, tiedetään, että ideaalin I virittää yksi alkio a, joka kuuluu johonkin yhdisteen ideaalieista $a \in I_t$, missä $1 \leq t \leq r$. Nyt ideaali $\langle a \rangle = I$ on pienin ideaali, joka sisältää alkion a, mutta myös ideaali I_t on pienin ideaali, joka sisältää alkion a. Siispä

$$\langle a \rangle = I = I_t \subseteq I_m \subseteq I$$

kaikilla $m \geq t$, mistä seuraa, että kaikilla $m \geq t$ pätee $I_m = I_t$. □

Jokainen rengas, jossa on äärellinen määrä alkiota, on noetherilainen. Myös jokainen kunta on Noetherin rengas, koska jokainen kunta on pääideaalialue korollaarin 3.14. mukaan.

Seuraavaksi käsitellään *Hilberin kantalausetta*, joka laajentaa tutkittavien Noetherin renkaiden määrää huomattavasti. Lauseen mukaan polynomirenkaat, joiden kerroinrengas on Noetherin rengas, ovat noetherilaisia. Hilbertin kantalauseen todistamista varten todistetaan ja määritellään ensiksi muutama aputulos. Seuraavassa lemmassa käytetään luvussa 2 määriteltyjä funktioita *kor* ja *deg.*

Lemma 5.8. *Olkoon R rengas ja $R[X]$ siitä muodostettu polynomirengas. Olkoon I renkaan $R[X]$ ideaali. Kaikilla kokonaisluvuilla $t \geq 0$ kerroinrenkaan R alkioista muodostettu joukko $I_t = \{kor(f) \mid f \in I, deg(f) \leq t\} \bigcup \{0\}$ on renkaan R ideaali.*

Todistus. Oletetaan, että t on epänegatiivinen kokonaisluku. Todistetaan ensiksi määritelmän 3.1. aliryhmäehdon ensimmäinen kohta eli, että ideaali I_t on vakaa yhteenlaskun suhteen. Tällöin kaikilla $a, b \in I_t$ täytyy päteä $a + b \in I_t$.

Olkoot $a, b \in I_t$. Tällöin $a = kor(f)$ ja $b = kor(g)$, joillakin polynomeilla $f, g \in I$, joiden aste on korkeintaan t. Olkoon $deg(f) = m$ ja $deg(g) = n$. Nyt polynomit ovat muotoa

$$f = ax^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

ja

$$g = bx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0.$$

Oletetaan, että $m \geq n$ ja määritellään uusi polynomi $h = f + x^{m-n}g$. Asteiden suuruuden järjestyksellä ei ole väliä, koska uusi polynomi voitaisiin määritellä sopivalla tavalla joka tapauksesssa. Koska polynomit f ja g kuuluvat ideaaliin I, myös $h \in I$ ja lisäksi huomataan, että

$$\begin{aligned} h &= (ax^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0) + x^{m-n}(bx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0) \\ &= (a+b)x^m + (a_{m-1}b_{n-1})x^{m-1} + \ldots. \end{aligned}$$

Koska $deg(h) = m \leq t$ ja $h \in I$, $kor(h) \in I_t$. Koska $kor(h) = a + b$, niin

$$a + b \in I_t.$$

Aliryhmän neutraalialkio 0 sisältyy joukkon I_t sen määritelmän mukaan. Osoitetaan vielä, että yhteenlaskun vasta-alkiot sisältyvät joukkoon I_t. Tämä seuraa siitä, että I on ideaali.

Olkoon $a = kor(f) \in I_t$. Nyt $f \in I$ ja $deg(f) \leq t$. Tällöin löytyy $-f \in I$, jolle pätee $deg(f) = deg(-f)$ ja $f + (-f) = f - f = 0$. Tästä seurauksena pätee

$$kor(f) + kor(-f) = 0.$$

Koska $-f \in I$ ja $deg(-f) \leq t$, niin $kor(-f) \in I_t$. Niinpä alkion $a \in I_t$ vasta-alkio $-a = kor(-f)$ kuuluu joukkoon I_t. Nyt joukko I_t on joukon R aliryhmä yhteenlaskun suhteen.

Todistetaan sitten määritelmän 3.1. toinen ehto, eli että kaikilla $r \in R$ ja $a \in I_t$ pätee $ar \in I_t$. Ehto $ar \in I_t$ riittää, koska tämän luvun renkaat on oletettu vaihdannaisiksi. Olkoon $a \in I_t$ ja $r \in R$. Tällöin $a = kor(f)$, jollakin polynomilla $f \in I$, jonka aste on korkeintaan t. Tutkitaan tuloa rf. Koska I on ideaali, pätee $rf \in I$ kaikilla $r \in R$. Lisäksi huomataan, että $deg(rf) = deg(f) \leq t$, koska r on vakio. Tällöin pätee $kor(rf) \in I_t$. Koska $ar = kor(rf)$, niin $ar \in I_t$ kaikilla $a \in I_t$ ja $r \in R$. Niinpä I_t on määritelmän 3.1. mukaan renkaan R ideaali. □

Nyt voidaan siirtyä Hilberin kantalauseen todistukseen.

Lause 5.9. *(Hilbertin kantalause) Noetherin renkaasta R muodostettu polynomirengas $R[X]$ on Noetherin rengas.*

Todistus. Olkoon I renkaan $R[X]$ satunnainen ideaali. Todistetaan, että ideali I on äärellisesti viritetty, mistä seuraa, että $R[X]$ on Noetherin rengas lauseen 5.4. mukaan.

Määritellään jokaista epänegatiivista kokonaislukua t kohti lemmasta 5.8. tuttu joukko

$$I_t = \{kor(f) \mid f \in I, deg(f) \leq t\} \bigcup \{0\}.$$

Nyt joukko I_t sisältää nolla-alkion ja ne renkaan R nollasta poikkeavat alkiot, jotka esiintyvät korkeimman asteen termin kertoimena jossakin ideaaliin I kuuluvassa polynomissa, jonka aste on korkeintaan t. Tällöin I_t on renkaan R ideaali (lemma 5.8.), jolle pätee $I_t \subseteq I_{t+1}$ kaikilla $t \geq 0$. Toisin sanoen kaikille ideaaleille I_t pätee

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots.$$

Koska R on Noetherin rengas, on olemassa kokonaisluku n, jolle pätee $I_t = I_n$ kaikilla $t \geq n$. Noetherilaisuudesta seuraa myös, että jokainen renkaan R ideaali on äärellisesti viritetty. Niinpä jokaista $t \geq 0$ kohden on olemassa alkiot $a_{t_1}, a_{t_2}, \ldots, a_{t_{k_t}}$, joille pätee

$$I_t = \langle a_{t_1}, a_{t_2}, \ldots, a_{t_{k_t}} \rangle.$$

Määritetään nyt ideaali J, joka koostuu renkaan $R[X]$ polynomeista. Valitaan jokaista kokonaislukua $0 \leq j \leq k_t$ kohden t-asteinen polynomi $f_{t_j} \in I$, jolle pätee $a_{t_j} = kor(f_{t_j})$. Olkoot polynomit f_{tj} ideaalin J virittäjiä kaikilla $t \leq n$. Tällöin ideaali J näyttää seuraavalta:

$$J = \langle f_{0_1}, \cdots, f_{0_{k_0}}, f_{1_1}, \cdots, f_{1_{k_1}}, \ldots, f_{n_1}, \cdots, f_{n_{k_n}} \rangle.$$

Osoitetaan seuraavaksi, että $J = I$. Tällöin I on äärellisesti viritetty, mistä seuraa, että $R[X]$ on noetherilainen.

Ideaalin J määritelmään mukaan kaikille $f \in J$ pätee $f \in I$, mistä seuraa, että

$$J \subseteq I.$$

Seuraavaksi osoitetaan toiseen suuntaan sisältyminen. Oletetaan, että f on polynomirenkaaseen $R[X]$ kuuluvan ideaalin I alkio. Osoitetaan polynomin f asteen t suhteen toisella induktioperiaatteella, että f kuuluu ideaaliin J.

Olkoon polynomi

$$f = bx^t + b_{t-1}x^{t-1} + \cdots + b_1x + b_0$$

renkaan $R[X]$ ideaalin I nollasta poikkeava alkio. Polynomin f aste on nyt t.

Induktion alkuaskel toteutuu, koska silloin kun polynomin f asteelle pätee $t = 0$, niin polynomi $f = b_0$. Tällöin f on vakiopolynomi, joka kuuluu ideaaliin I_0, koska $f \in I$. Ideaalin J määritelmän mukaan $I_0 \subseteq J$, koska ideaalin J virittäjät valittiin niistä ideaalin I polynomeista, joiden korkeimman asteen termien kertoimet kuuluuvat aina oman asteensa t ideaaliin I_t virittäjäalkiohin. Tässä tapauksessa $b_0 = kor(f_{0_j})$, jollakin $0 \leq j \leq k_0$.

Oletetaan seuraavaksi, että mikä tahansa polynomi $f \in I$, jonka aste on korkeintaan $t-1$ kuuluu ideaaliin J. Osoitetaan, että tästä seurauksena mikä tahansa t-asteinen polynomi $f \in I$ kuuluu ideaalin J. Tällöin toisen induktioperiaattteen nojalla jokainen ideaalin I polynomi f kuuluu joukkoon J. Jaetaan induktioaskeleen $f \in J$, kun $deg(f) = t$ todistaminen kahteen osaan. Toisessa oletetaan, että $t > n$ ja toisessa, että $t \leq n$.

Siinä tapauksessa, että polynomin asteelle pätee $t > n$, polynomin f korkeimman asteen termin kerroin $b = kor(f)$ kuuluu ideaalin I_n, koska $I_t = I_n$ kaikilla $t > n$ ja $f \in I$. Nyt kerroin b saadaan kirjoitettua ideaalin I_n virittäjien lineaarikombinaationa

$$b = a_{n1}c_1 + a_{n2}c_2 + \cdots + a_{nk}c_k,$$

joillakin alkioilla $c_1, c_2, \ldots, c_k \in R$. Lisäksi tiedetään, että polynomi

$$g = f - (f_{n1}c_1 + f_{n2}c_2 + \cdots + f_{nk}c_k)x^{t-n}$$

kuuluu ideaaliin I, koska $f \in I$, kaikki $f_{n_1}, f_{n_2}, \cdots \in I$ ja $x^{t-n} \in R[X]$. Polynomin g aste on matalampi kuin t, koska t-asteisen termin kerroin on erotuksen mukaan nolla

$$b - (a_{n1}c_1 + a_{n2}c_2 + \cdots + a_{nk}c_{m_n}) = 0.$$

Tästä seuraa, että induktio-oletuksen perusteella $g \in J$. Lisäksi tiedetään, että kaikki $f_{n_1}, f_{n_2} \cdots \in J$ ja $x^{t-n} \in R[X]$. Niinpä termi $(f_{n1}c_1 + f_{n2}c_2 + \cdots + f_{nk}c_k)x^{t-n} \in J$. Siten myös $f \in J$ ideaalin määritelmän mukaan, koska $f = g + (f_{n1}c_1 + f_{n2}c_2 + \cdots + f_{nk}c_k)x^{t-n}$.

Kun polynomin asteelle pätee $t \leqslant n$ polynomin korkeimman asteen termin kerroin $b = kor(f)$ kuuluu ideaaliin I_t, koska $f \in I$. Tällöin b voidaan kirjoittaa ideaalin I_t virittäjien lineaarikombinaationa

$$b = a_{t1}d_1 + a_{t2}d_2 + \cdots + a_{tk}d_k$$

joillakin alkioilla $d_1, d_2, \ldots, d_k \in R$. Lisäksi tiedetään, että polynomi

$$h = f - (f_{t1}d_1 + f_{t2}d_2 + \cdots + f_{tk}d_k)$$

kuuluu ideaaliin I, koska $f \in I$ ja kaikki $f_{t_1}, f_{t_2}, \cdots \in I$. Nyt polynomin h aste on matalampi kuin t, koska samaan tapaan t-asteisen termin kerroin on erotuksen mukaan taas nolla

$$b - (a_{t1}d_1 + a_{t2}d_2 + \cdots + a_{tk}d_k) = 0.$$

Niinpä $h \in J$ induktio-oletuksen perusteella. Koska myös termi $(f_{t1}d_1 + f_{t2}d_2 + \cdots + f_{tk}d_k)$ kuuluu ideaaliin J, niin $f = h + (f_{t1}d_1 + f_{t2}d_2 + \cdots + f_{tk}d_k) \in J$ ideaalin määritelmän mukaan.

Koska induktio-oletuksesta $f \in J$, kun $deg(f) \leq t-1$ seuraa, että induktioaskel $f \in J$, kun $deg(f) = t$ pätee, niin $f \in J$ kaikilla polynomeilla $f \in I$.

Niinpä aina kun f kuuluu ideaaliin I, niin f kuuluu idealiin J. Tästä seuraa

$$I \subseteq J.$$

Koska ideaaleille I ja J pätee $I \subseteq J$ ja $J \subseteq I$, niin $I = J$. Niinpä polynomirenkaan $R[X]$ yleinen ideaali I on äärellisesti viritetty ja siten rengas $R[X]$ on lauseen 5.4. mukaan noetherilainen.

□

Hilbertin kantalauseen seurauksena monet polynomilaajennokset ovat noetherilaisia. Esimerksiksi okonaisluvuista sekä kunnista muodostetut polynomirenkaat, joissa on äärellinen määrä tuntemattomia ovat noetherilaisia.

Noetherin renkaat toteuttavat nousevan ketjun ehdon. Näissä renkaissa mikään ideaaliketju ei voi kasvaa äärettömästi. Noetherin renkaiden ei tarvitse kuitenkaan toteuttaa *laskevan ketjun ehtoa*. Seuraavaksi tutkitaan renkaita, joiden ideaalit toteuttavat laskevan ketjun ehdon. Laskevan ketjun ehdon renkaissa mikään ideaaliketju ei voi supeta äärettömästi. Tällaisia renkaita kutsutaan *Artinin renkaiksi* matemaatikko Emil Artinin (1898−1962) mukaan.

Määritelmä 5.10. Rengas R toteuttaa *laskevan ketjun ehdon*, jos mitä tahansa renkaan ideaaleja

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \ldots$$

kohden on olemassa kokonaisluku n, siten että kaikilla $m \geq n$ pätee $I_m = I_n$.

Määritelmä 5.11. Rengas, joka toteuttaa laskeven ketjun ehdon on *Artinin rengas*. Voidaan puhua myös renkaasta, joka on *artinilainen*.

Määritelmä 5.12. Rengas R toteuttaa *ideaalien minimiehdon*, jos kaikilla renkaan R epätyhjillä ideaaleista koostuvilla (sisältymisen mukaan järjestetyillä) joukoilla on minimialkio. Toisin sanoen renkaan sisäiset ideaaliketjut suppenevat vain tiettyyn minimialkioon asti.

Määritelmät 5.12., 5.13. ja 5.14. ovat ekvivalentteja. Siispä Artinin renkaissa toteutuu sekä laskevan ketjun ehto, että ideaalien minimiehto. Todistetaan seuraavaksi, että rengas, joka toteuttaa ideaalien minimiehdon, on artinilainen.

Lause 5.13. *Rengas R on artinilainen, jos ja vain jos se toteuttaa ideaalien minimiehdon eli määritelmän 5.14.*

Todistus. Todistetaan ensiksi, että jos rengas R on artinilainen, se toteuttaa ideaalien minimiehdon. Oletetaan siis, että R on Artinin rengas ja F epätyhjä joukko renkaan R ideaaleja.

Oletetaan, että joukolla F ei ole minimialkiota. Toisin sanoen joukko F ei toteuta määritelmää 5.14. Olkoon I_1 renkaan R ideaali, joka kuuluu joukkoon F. Koska I_1 ei ole joukon F minimialkio, on olemassa toinen ideaali $I_2 \in F$, jolle pätee $I_1 \supset I_2$. Koska I_2 ei ole joukon F minimialkio, on olemassa ideaali $I_3 \in F$, jolle pätee $I_2 \supset I_3$. Tätä päättelyä jatkamalla saadaan loputtomasti jatkuva laskevien ideaalien ketju

$$I_1 \supset I_2 \supset I_3 \dots .$$

Tämä on ristiriidassa alkuoletuksen R on artinilainen suhteen. Artinin renkaiden ideaaliketjut eivät voi supeta äärettömästi. Niinpä joukolla F on oltava minimialkio. Tällöin F toteuttaa ideaalien minimiehdon.

Todistetaan nyt toinen suunta. Jos rengas R toteutaa ideaalien minimiehdon, se on Artinin rengas.

Oletetaan, että rengas R toteuttaa määritelmän 6.3. eli jokaisella renkaan ideaaliketjulla on jokin minimialkio. Olkoon $I_1 \supseteq I_2 \supseteq I_3 \dots$ laskeva ketju renkaan R ideaaleja. Tutkitaan nyt renkaan R ideaaleista koostuva joukkoa

$$F = \{I_t \mid t = 1, 2, 3, \dots\}.$$

Koska R toteuttaa ideaalien minimiehdon, joukolla F on minimialkio I_n, missä n on jokin positiivinen kokonaisluku. Tällöin joukon F ideaaleille pätee $I_m \subseteq I_n$ kaikilla $m \geq n$. Oletetaan nyt, että pätee $I_m \neq I_n$, mistä seuraa, että $I_m \subset I_n$. Koska joukon F minimialkio on I_n, niin $I_m \notin F$, mikä johtaa ristiriitaan. Niinpä $I_m = I_n$ kaikilla $m \geq n$. Koska renkaan R laskevien ideaalien ketju stabiloituu aina minimialkioon, R on artinilainen.

□

Aiemmin käsitelty kokonaislukurengas $\mathbb{Z}$, joka paljastui Noetherin alueeksi, ei ole artinilainen. Kokonaislukujen joukossa on äärettömiä laskevia ideaaliketjuja, esimerkiksi

$$\langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \dots .$$

Tästä johtuen kokonaislukujen joukko $\mathbb{Z}$ ei ole artinilainen.

Aiemmin määriteltiin Noetherin alue noetherilaiseksi kokonaisalueeksi. Seuraavaksi määritellään samalla tavoin *Artinin alue*.

Määritelmä 5.14. Kokonaisalue, jossa pätee laskevan ketjun ehto, on *Artinin alue*.

Artinin alue on siis kokonaisalue, jossa pätee laskevan ketjun ehto ja ideaalien minimiehto.

Luku 6

Ketjuehtorenkaiden ominaisuuksia

Tässä luvussa käsitellään ketjuehtorenkaiden yleisiä tuloksia. Luvussa todistetaan, että jokainen Artinin alue on kunta. Tämän lisäksi luvussa jatketaan neljännessä luvussa aloitettua tekijöihinjaon alueiden tutkimista. Tässä luvussa todistetaan, että jokainen Noetherin alue on tekijöihinjaon alue. Tämän avulla päästään todistamaan, että jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue. Luvun tärkeimmät lähteet ovat [1], [4] ja [6].

Lause 6.1. *Jokainen Artinin alue on kunta.*

Todistus. Olkoon R Artinin alue ja $a \neq 0$ alueen R alkio. Koska alue R on artinilainen, laskevien ideaalien ketjulla

$$\langle a \rangle \supseteq \langle a^2 \rangle \supseteq \langle a^3 \rangle \supseteq \cdots \supseteq \ldots$$

on indeksi n, jonka jälkeen ideaalit eivät enää pienene. Toisin sanoen

$$\langle a^n \rangle = \langle a^{n+1} \rangle = \langle a^{n+2} \rangle \ldots$$

Tästä seuraa, että

$$a^n = ra^{n+1},$$

jollakin $r \in R$. Edellisestä yhtälöstä voidaan supistaa a^n, koska $a^n \neq 0$. Tällöin päästään tulokseen

$$1 = ra,$$

mistä seuraa, että a:lla on käänteisalkio. Niinpä alueen R nollasta poikkeava alkio a on kääntyvä. Nyt määritelmän 2.6. nojalla Artinin alue R on kunta. □

Korollaari 6.2. *Lauseen 6.3. seurauksena jokainen kokonaisalue, jossa on äärellinen määrä ideaaleja, on kunta.*

Tätä tulosta sivuttiin jo kokonaisalueen ja kunnan esittelyssä toisessa luvussa.

Lause 6.3. *Jokainen Noetherin alue on tekijöihinjaonalue.*

Todistus. Oletetaan, että R on Noetherin alue, joka ei ole tekijöihinjaonalue. Tällöin kokonaisalueessa R on olemassa vähintään yksi nollasta poikkeava alkio a, joka ei ole kääntyvä, ja joka ei voi olla renkaan R jaottomien alkioiden äärellinen tulo. Olkoon X joukko, joka koostuu a:n kaltaisista alkioista. Koska ainkain alkio $a \in X$, joukko X ei voi olla tyhjä. Määritellään nyt joukko

$$S = \{\langle x \rangle \mid x \in X\},$$

eli S on alueen R ideaaleista koostuva epätyhjä joukko. Koska R on noetherilainen, joukolla S on maksimialkio $\langle m \rangle$. Nyt $m \in X$, eli m ei ole jaoton. Niinpä $m = cd$, joillakin ei-kääntyvillä nollasta poikkeavilla alkiolla $c, d \in R$. Tästä seuraa, että

$$\langle m \rangle \subset \langle c \rangle, \langle m \rangle \subset \langle d \rangle$$

ja edelleen

$$\langle c \rangle, \langle d \rangle \notin S,$$

koska $\langle m \rangle$ on joukon maksimialkio. Seurauksena renkaan R alkiot c ja d sekä eritoten $m = cd$ ovat alueen R jaottomien alkioiden äärellisiä tuloja. Tästä seuraa ristiriita, koska alkio m kuuluu joukkoon X, eli joukkoon, jonka alkiot eivät ole jaottomien alkioiden äärellisiä tuloja. Niinpä Noetherin alue R on tekijöihinjaonalue. □

Korollaari 6.4. *Lauseiden 5.7. ja 6.3. seurauksena jokainen pääideaalialue on tekijöihinjaonalue.*

Jatketaan korollaarin 6.4. tulosta ja näytetään vielä toteen, että jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue. Todistuksesta puuttuu enää tieto, että jokaisen alkion tekijöihinjako on yksikäsitteinen.

Lause 6.5. *Jokainen pääideaalialue D on yksikäsitteisen tekijöihinjaon alue.*

Todistus. Olkoon D pääideaalialue ja $a \neq 0$ alueen D ei-kääntyvä alkio. Korollaarin 6.4. nojalla D on tekijöihinjaon alue. Oletetaan, että a voidaan kirjoittaa kahdella eri tapaa jaottomien alkioiden tulona:

$$a = p_1 p_2 \dots p_n$$

$$a = q_1 q_2 \dots q_m,$$

missä jokainen p_i ja q_j on jaoton sekä $m \geq n$. Nyt, koska p_1 on alkualkio (lause 4.9.3.), tulo $q_1 q_2 \dots q_m$ on jaollinen luvulla p_1 ja edelleen $p_1 | q_j$, jollain $j \in \mathbb{N}$. Muuttamalla sopivasti tulon $q_1 q_2 \dots q_m$ alkioiden järjestystä saadaan, että

$$p_1 | q_1.$$

Tällöin

$$q_1 = u_1 p_1,$$

jollain yksiköllä $u_1 \in D$. Nyt sijoittamalla edellinen tulos a:n lausekkeeseen saadaan

$$a = p_1 p_2 \dots p_n = u_1 p_1 q_2 \dots q_m,$$

mistä seuraa, että

$$p_2 \dots p_n = u_1 q_2 \dots q_m.$$

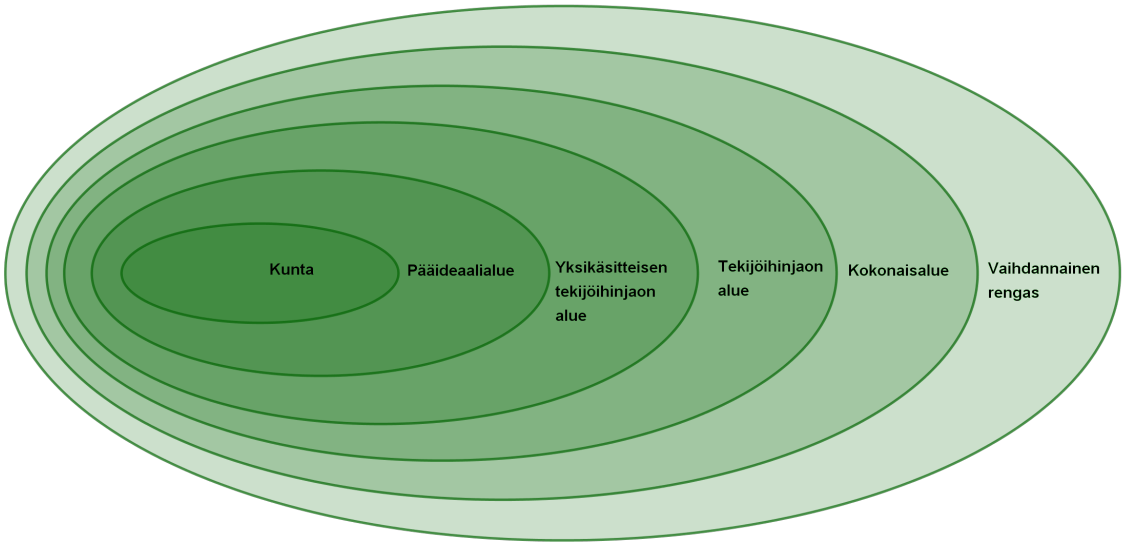
Tätä menetelmää jatkamalla päädytään lopulta tulokseen

$$1 = u_1 u_2 \dots u_n q_{n+1} \dots q_m.$$

Jos pätee $m > n$, niin päädytään ristiriitaan, sillä tuloon jäisi vähintään yksi q_j, joka olisi yksikkö. Niinpä täytyy päteä $n = m$, eli jaottomien alkioiden määrä on sama. Lisäksi alkiot $p_1, p_2, \dots, p_m$ ovat alkioiden $q_1, q_2, \dots, q_m$ liittolukuja jollain järjestyksellä. Niinpä alkion a alkuhajotelma on yksikäsitteinen ja edelleen D on yksikäsitteisen tekijöihinjaon alue. □

Yksikäsitteisen tekijöihinjaon alue on siten pääideaalialuetta yleisempi käsite, sillä kuten äsken todistettiin jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue. Esimerkiksi luvussa 4 huomattiin, että kokonaislukujen joukko $\mathbb{Z}$ on sekä pääideaalialue että yksikäsitteisen tekijöihinjaon alue. Jokainen yksikäsitteisen tekijöihinjaon alue ei kuitenkaan ole pääideaalialue. Esimerkiksi $\mathbb{Z}[X]$ on korollaarin 5.10. ja lauseen 6.3. nojalla yksikäsitteisen tekijöihinjaon alue. Toisaalta renkaan $\mathbb{Z}[X]$ ideaali $(2, x)$ ei ole pääideaali, koska se ei ole yhden alkion virittämä. Niinpä rengas $\mathbb{Z}[X]$ ei ole pääideaalialue.

Tutkielmassa ollaan selvitetty monia rakenteiden sisäiseen sisältymisjärjestykseen liityviä tuloksia. Kootaan seuraavaksi käsiteltyjä rakenteita sisältymisen mukaan järjestettynä kuvaan.



Noetherin alueet sijoittuvat tekijöihinjaon alueiden ja pääideaalialueiden väliin. Noetherin alueita ei ole yllä olevassa kuvassa, koska Noetherin alueiden yhteys yksikäsitteisen tekijöihinjaon alueisiin ei ole sisältymisen mukaan selkeä. Kaikki yksikäsitteisen tekijöihinjaon alueet eivät ole noetherilaisia, eivätkä kaikki Noetherin alueet ole yksikäsitteisen tekijöihinjaon alueita.

Lisäksi tiedetään, että jokainen Artinin alue on kunta. Artinin alueet eivät välttämättä ole kuitenkaan pääideaalialueita, joten nekään eivät sovi yllä olevaan kuvaan.

Kirjallisuutta

[1] M.R. Adhikari, A. Adhikari: Basic Modern Algebra with Applications, Springer India, 2014.

[2] Jokke Häsä, Johanna Rämö: Johdatus abstraktiin algebraan , 3. painos, Gaudeamus, 2015.

[3] Serge Lang: Algebraic Structures, 2nd edition, Addison-Wesley Publishing Company, 1968.

[4] Serge Lang: Algebra, 5th edition, Addison-Wesley, 1965.

[5] Murray R. Spiegel: Schaum's outline of Theory and Problems of Complex Variables, 32th edition McGraw-Hill, 1964.

[6] John B. Fraleigh: A First Course in Abstract Algebra, 7th edition, Pearson Education; Dorling Kindersley, 1967.

[7] I, N Herstein: Topics in Algebra, Blaisdell, 1964.